

ArubaOS 8.x Command-Line Interface

aruba

a Hewlett Packard
Enterprise company

Reference Guide

Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

Following lists the updates to the ArubaOS CLI:

- [ArubaOS 8.11.1.0](#)
- [ArubaOS 8.11.0.0](#)
- [ArubaOS 8.10.0.0](#)
- [ArubaOS 8.9.0.0](#)
- [ArubaOS 8.8.0.0](#)
- [ArubaOS 8.7.0.0](#)
- [ArubaOS 8.6.0.0](#)
- [ArubaOS 8.5.0.0](#)
- [ArubaOS 8.4.0.0](#)
- [ArubaOS 8.3.0.0](#)
- [ArubaOS 8.2.2.0](#)
- [ArubaOS 8.2.1.0](#)
- [ArubaOS 8.2.0.0](#)
- [ArubaOS 8.1.0.0](#)
- [ArubaOS 8.0.1.0](#)

This guide describes the ArubaOS 8.x commands. The commands in this guide are listed alphabetically. The following information is provided for each command:

- **Command Syntax**—The complete syntax of the command.
- **Description**—A brief description of the command, including usage guidelines, prerequisites, prohibitions, and related commands.
- **Example**—An example of how to execute the command.
- **Command History**—The version of ArubaOS 8.x in which the command was first introduced, including the modification history.
- **Command Information**—This table describes any licensing requirements, command modes and platforms for which this command is applicable. For more information about available licenses, refer to the *Aruba Mobility Conductor Licensing Guide*.

Connecting to the Mobility Conductor or Managed Device

This section describes how to connect to the Mobility Conductor or Managed Device to use the CLI.

Serial Port Connection

The serial port is located on the front panel of the managed device. Connect a terminal or PC or workstation running a terminal emulation program to the serial port on the managed device to use the CLI. Configure your terminal or terminal emulation program to use the following communication settings.

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None



The Aruba 7200 Series controller supports baud rates between 9600 and 115200.

Telnet or SSH Connection

Telnet or SSH access requires that you configure an IP address and a default gateway on Mobility Conductor/Managed Device and connect the Mobility Conductor/Managed Device to your network. This is typically performed when you run the initial setup on the Mobility Conductor/Managed Device, as described in the *ArubaOS 8.x Quick Start Guide*. In certain deployments, you can also configure a loopback address for the Mobility Conductor/Managed Device; see [interface loopback on page 749](#) for more information.

Configuration changes on Mobility Conductor

Some commands can only be issued when connected to Mobility Conductor. If you make a configuration change on Mobility Conductor, all connected managed devices using that configuration will subsequently update their settings as well.

CLI Access

When you connect to the Mobility Conductor using the CLI, the system displays the login prompt. Log in using the admin user account and the password you entered during the initial setup on the Mobility Conductor . For example:

```
login as: admin
admin@192.0.2.1's password:
Last login: Sat Jun 25 01:17:11 2016 from 192.0.2.77
```

When you are logged in, the *enable* mode CLI prompt displays. For example:

```
(host) [mynode] #
```

All **show** commands and certain management functions are available in the enable (also called “privileged”) mode.

Configuration commands are available in *config* mode. Move from enable mode to config mode by entering **configure terminal** at the # prompt:

```
(host) [mynode]# configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

When you are in basic config mode, (config) appears before the # prompt:

```
(host) [mynode] (config) #
```



There are several other sub-command modes that allow users to configure individual interfaces, sub-interfaces, loopback addresses, GRE tunnels and cellular profiles. For details on the prompts and the available commands for each of these modes, see [Command Modes on page 7](#).

Command Help

You can use the question mark (?) to view various types of command help.

When typed at the beginning of a line, the question mark lists all the commands available in your current mode or sub-mode. A brief explanation follows each command. For example:

```
(host) [mynode] #aaa ?
authentication      Authentication
inservice           Bring authentication server into service
ipv6                Internet Protocol Version 6
query-user          Query User
test-server         Test authentication server
user                User commands
```

When typed at the end of a possible command or abbreviation, the question mark lists the commands that match (if any). For example:

```
(host) [mynode] #c?  
ccm-debug          Centralized Configuration Module debug information  
cd                 Change current config node  
change-config-node Change current config node  
clear              Clear configuration  
clock              Append clock to cli output  
cluster-debug      Cluster Debug  
configure          Configuration Commands  
copy               Copy Files  
copy-provisioning-par.. Copy a provisioning-ap-list entry to provisioning-params  
crypto             Configure IPsec, IKE, and CA
```

If more than one item is shown, type more of the keyword characters to distinguish your choice. However, if only one item is listed, the keyword or abbreviation is valid and you can press tab or the spacebar to advance to the next keyword.

When typed in place of a parameter, the question mark lists the available options. For example:

```
(host) [mynode] #write ?  
erase              Erase and start from scratch  
memory             Write to memory  
terminal           Write to terminal  
<cr>
```

The <cr> indicates that the command can be entered without additional parameters. Any other parameters are optional.

Command Completion

To make command input easier, you can usually abbreviate each key word in the command. You need type only enough of each keyword to distinguish it from similar commands. For example:

```
(host) [mynode] #configure terminal
```

could also be entered as:

```
(host) [mynode] #con t
```

Three characters (**con**) represent the shortest abbreviation allowed for **configure**. Typing only **c** or **co** would not work because there are other commands (like **copy**) which also begin with those letters. The configure command is the only one that begins with **con**.

As you type, you can press the spacebar or tab to move to the next keyword. The system then attempts to expand the abbreviation for you. If there is only one command keyword that matches the abbreviation, it is filled in for you automatically. If the abbreviation is too vague (too few characters), the cursor does not advance and you must type more characters or use the help feature to list the matching commands.

Deleting Configuration Settings

Use the **no** command to delete or negate previously-entered configurations or parameters.

- To view a list of no commands, type **no** at the enable or config prompt followed by the question mark. For example:

```
(host) [mynode] (config) # no?
```

- To delete a configuration, use the **no** form of a configuration command. For example, the following command removes a configured user role:

```
(host) [mynode] (config) # no user-role <name>
```

- To negate a specific configured parameter, use the **no** parameter within the command. For example, the following commands delete the DSCP priority map for a priority map configuration:

```
(host) [mynode] (config) # priority-map <name>
(host) [mynode] (config-priority-map) # no dscp priority high
```

Command Modes

The ArubaOS CLI offers different levels of user access by differentiating between different command modes.

When you first log in to the CLI, you start your session in *User* mode, which provides only limited access for basic operational testing. You must enter an additional password to access *Enable* mode, which allows you to issue show commands run certain management functions. Configuration commands can only be issued in *Configuration* mode. You can access Config mode by entering **configure terminal** at the command prompt. You can exit your current command mode and return to a lower-level command mode at any time by entering **exit** at the command prompt.

The following sections describes how to access each command mode, the command prompt for each mode, and links to its available commands:

- [Enable Mode on page 7](#)
- [Config Mode on page 8](#)

Enable Mode

On logging onto the Mobility Conductor, the user mode is presented.

The command prompt for a CLI session in enable mode is a pound (**#**) symbol:

```
(host) [mynode] #
```

To view a list of commands available in enable mode, access the CLI in enable mode and enter a question mark (?):

```
(host) [mynode]#?
```

Some top-level commands have different sets of sub-commands available in Enable or Config mode. To view a list of available sub-commands in Enable mode, access the CLI in Enable mode, enter the top

level command, then enter a question mark (?). For example, the following example shows which aaa commands are available in Enable mode:

```
(host) [mynode]#aaa ?
authentication      Authentication
inservice           Bring authentication server into service
ipv6                Internet Protocol Version 6
query-user          Query User
test-server         Test authentication server
user                User commands
```

Config Mode

To move from enable mode to config mode, enter the command **config terminal**. Users in config mode may return to enable mode at any time by entering the command **exit**.

When you are in config mode, **(config)** appears before the # prompt:

```
(host) [mynode] (config) #
```

Some top-level commands have different sets of sub-commands available in the Enable or Config mode. To view a list of available sub-commands in the Config mode, access the CLI in the Config mode, enter the top level command, then enter a question mark (?). For example, the following example shows which **aaa** commands are available in the Config mode:

```
(host) [mynode] (config) #aaa ?
alias-group          Configure an Alias Group
auth-survivability   Configure Auth Survivability
auth-trace           Set parameters for debug tracing in AUTH (light weight
tracing)
authentication       Authentication
authentication-server Authentication Servers
bandwidth-contract   Configure bandwidth contract (256 Kbps - 2 Gbps)
derivation-rules     Configure rules to derive user role or vlan
dns-query-interval   Set DNS query interval
log                  Enable debugging on per-user basis
password-policy      Password policy for locally configured management users
profile              Configure an AAA Profile
radius-attributes    Configure RADIUS attribute
rfc-3576-server      Configure an RFC 3576 Server
server-group         Configure a Server Group
tacacs-accounting    Configure accounting
timers               Configure authentication timers
user                 User commands
xml-api              External XML API server
```

Configuration Sub-modes

Some Config mode commands can enter you into a sub-mode with a limited number of available commands specific to that mode. When you are in a configuration sub-mode, the (config) that appears before the command prompt will change to indicate your current mode; e.g (config-submode).

You can exit a sub-command mode and return to the basic configuration mode at any time by entering the [exit](#) command.

Saving Configuration Changes

Mobility Conductor has the running configuration images. The *running-config* holds the current controller configuration, including all pending changes which have yet to be saved. To view the running-config, use the following command:

```
(host) [mynode]# show running-config
```

When you make configuration changes via the CLI, those changes affect the current running configuration only. If the changes are not saved, they will be lost after the Mobility Conductor reboots. To save your configuration changes so they are retained after the Mobility Conductor reboots, use the following command in the enable or config mode:

```
(host) ^[mynode]# write memory
Saving Configuration...
Saved Configuration
```

The running configuration can also be saved to a file or sent to a TFTP server for backup or transfer to another system.

The ^ indicator appears between the (host) and [node] portions of the command prompt if the configuration contains unsaved changes. ArubaOS includes the following command prompts:

- (host) ^[mynode] – This indicates unsaved configuration.
- (host) *[mynode] – This indicates available crash information.
- (host) [mynode] – This indicates a saved configuration.

Commands That Reset the Mobility Conductor or AP

If you use the CLI to modify a currently provisioned and running radio profile, those changes take place immediately; you do not reboot the Mobility Conductor or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the Mobility Conductor or AP to reboot. You may want to consider current network loads and conditions before issuing these commands, as they may cause a momentary disruption in service as the unit resets. Note also that changing the **lms-ip** parameter in an AP system profile associated with an AP group will cause all APs in that AP group to reboot.

Table 1: *Reset Commands*

Commands that Reset an AP	Commands that Reset a Mobility Conductor
<ul style="list-style-type: none">▪ ap-regroup▪ ap-rename▪ apboot▪ provision-ap▪ ap wired-ap-profile {default <profile-name>} forward-mode {bridge split-tunnel tunnel}▪ wlan virtual-ap <profile-name> {aaa-profile <profile-name> forward-mode {tunnel bridge split-tunnel decrypt-tunnel} ssid-profile <profile-name> vlan <vlan>...}	<ul style="list-style-type: none">▪ reload

Commands that Reset an AP	Commands that Reset a Mobility Conductor
<ul style="list-style-type: none"> ▪ <code>ap system-profile <profile-name> {bootstrap-threshold <number> lms-ip <ipaddr> }</code> ▪ <code>wlan ssid-profile <profile-name> {battery-boost deny-bcast essid opmode strict-svp wepkey1 <key> wepkey2 <key> wepkey3 <key> wepkey4 <key> weptxkey <index> wmm wmm-be-dscp <best-effort> wmm-bk-dscp <background> wmm-ts-min-inact-int <milliseconds> wmm-vi-dscp <video> wmm-vo-dscp <voice> wpa-hexkey <psk> wpa-passphrase <string> }</code> ▪ <code>wlan dot11k <profile-name> {bcn-measurement-mode dot11k-enable force-dissasoc }</code> 	

Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 2: Text Conventions

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
Boldface	This style is used to emphasize command names and parameter options when mentioned in the text.
Commands	This fixed-width font depicts command syntax and examples of commands and command output.
<angle brackets>	In the command syntax, text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: ping <ipaddr> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.
[square brackets]	In the command syntax, items enclosed in brackets are optional. Do not type the brackets.
{Item_A Item_B}	In the command examples, single items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

Type Style	Description
<code>{ap-name <ap-name>} {ipaddr <ip-addr>}</code>	Two items within curled braces indicate that both parameters must be entered together. If two or more sets of curled braces are separated by a vertical bar, like in the example to the left, enter only one choice Do not type the braces or bars.

Command Line Editing

The system records your most recently entered commands. You can review the history of your actions, or reissue a recent command easily, without having to retype it.

To view items in the command history, use the *up* arrow key to move back through the list and the *down* arrow key to move forward. To reissue a specific command, press **Enter** when the command appears in the command history. You can even use the command line editing feature to make changes to the command prior to entering it. The command line editing feature allows you to make corrections or changes to a command without retyping. [Table 3](#) lists the editing controls. To use key shortcuts, press and hold the **Ctrl** button while you press a letter key.

Table 3: Line Editing Keys

Key	Effect	Description
Ctrl A	Home	Move the cursor to the beginning of the line.
Ctrl B or the left arrow	Back	Move the cursor one character left.
Ctrl D	Delete Right	Delete the character to the right of the cursor.
Ctrl E	End	Move the cursor to the end of the line.
Ctrl F or the right arrow	Forward	Move the cursor one character right.
Ctrl K	Delete Right	Delete all characters to the right of the cursor.
Ctrl N or the down arrow	Next	Display the next command in the command history.
Ctrl P or up arrow	Previous	Display the previous command in the command history.
Ctrl T	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
Ctrl U	Clear	Clear the line.
Ctrl W	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
Ctrl X	Delete Left	Delete all characters to the left of the cursor.

Specifying Addresses and Identifiers in Commands

This section describes addresses and other identifiers that you can reference in CLI commands.

Table 4: *Addresses and Identifiers*

Address or Identifier	Description
IP address	For any command that requires an IP address to specify a network entity, use IPv4 network address format in the conventional dotted decimal notation (for example, 10.4.1.258).
Netmask address	For subnet addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
MAC address	For any command that requires a device's hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
SSID	A unique character string (sometimes referred to as a network name), consisting of not more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).
BSSID	This entry is the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g— used from the AP. Use the same format as that of a MAC address.
ESSID	The unique logical name of a wireless network. If the ESSID includes spaces, you must enclose the name in quotation marks.
Fast Ethernet or Gigabit Ethernet interface	Any command that references a Fast Ethernet or Gigabit Ethernet interface requires that you specify the corresponding port on the managed device in the format <slot>/<module>/<port>: Use the show port status command to obtain the interface information currently available from a managed device.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 5: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.arubanetworks.com/
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

aaa alias-group

```
aaa alias-group <ag-name>
  clone <group>
  no ...
  set
    vlan
      condition {ssid | location} equals <operand> set-value <set-value-string>
```

Description

This command configures a AAA alias with set of VLAN derivation rules that could speed up user rule derivation processing for deployments with a very large number of UDRs.

Parameter	Description
<ag-name>	Name of the alias group.
clone <group>	Copy data from another alias group.
no	Delete command.
set	Configure rules to derive role or VLAN.
vlan	Configure rule to set VLAN.
condition	Select one of the following condition to be matched: <ul style="list-style-type: none">▪ ssid : ESSID of the access point.▪ location : user location (ap name)
equals <operand>	Check if condition set equals the operand value.
set-value <set-value-string>	Specify the value that the role or VLAN should be set to.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication captive-portal

```
aaa authentication captive-portal <profile>
  apple-cna-bypass
  ap-mac-in-redirectation-url
  auth-protocol mschapv2|pap|chap
  black-list/deny-list <black-list>/<deny-list>
  clone <source-profile>
  default-guest-role <role>
  default-role <role>
  enable-welcome-page
  guest-logon
  ip-addr-in-redirectation <ipaddr>
  login-page <url>
  logon-wait {cpu-threshold <percent>}|{maximum-delay <seconds>}|{minimum-delay
  <seconds>}
  logout-popup-window
  max-authentication-failures <number>
  no ...
  protocol-http
  proxy <ipaddr> port <port>
  redirect-pause <seconds>
  redirect-url <url>
  server-group <group-name>
  show-acceptable-use-policy
  show-fqdn
  single-session
  switchip-in-redirectation-url
  url-hash-key <key>
  user-idle-timeout
  user-logon
  user-vlan-in-redirectation-url
  welcome-page <url>
  white-list/allow-list <white-list>/<allow-list>
```

Description

This command configures the Captive Portal authentication profile in the base operating system or with the PEFNG license installed. When you configure the profile in the base operating system, the name of the profile must be entered for the initial role in the AAA profile. Also, when you configure the profile in the base operating system, you cannot define the default-role.

Starting from ArubaOS 8.7.0.0, captive portal authentication is supported for VAPs in the bridge forwarding mode. Only the following parameters of the `aaa authentication captive-portal` command will be supported in the bridge forwarding mode:

- `ap-mac-in-redirectation-url`
- `ip-addr-in-redirectation-url`
- `login-page`
- `switchip-in-redirectation-url`
- `url-hash-key`
- `user-vlan-in-redirectation-url`

Parameter	Description
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters. default
apple-cna-bypass	Enable this knob to bypass Apple CNA on iOS devices such as iPad, iPhone, and iPod. You need to perform Captive Portal authentication from browser.
authentication-protocol chap mschapv2 pap	This parameter specifies the type of authentication required by this profile, PAP is the default authentication type. mschapv2, pap, chap pap
ap-mac-in-redirection-url	This parameter adds the AP's MAC address in the redirection URL. disabled
black-list/deny-list	Name of an existing blacklist/denylist on an IPv4 or IPv6 network destination. The blacklist/denylist contains websites (unauthenticated) that a guest cannot access. Specify a netdestination host or subnet to add that netdestination to the captive portal blacklist/denylist. If you have not yet defined a netdestination, use the netdestination command to define a destination host or subnet before you add it to the blacklist/denylist.
clone	Name of an existing Captive Portal profile from which parameter values are copied.
default-guest-role	Role assigned to guest. guest
default-role <role>	Role assigned to the Captive Portal user when that user logs in. When both user and guest logons are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role. guest
enable-welcome-page	Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, redirection to the web URL happens immediately after the user logs in. enabled
guest-logon	Enables Captive Portal logon without authentication. disabled
ipaddr-in-redirection-url	Sends the interface IP address of the managed device in the redirection URL when external captive portal servers are used. An external captive portal server can determine the managed device from which a request originated by parsing the switchip variable in the URL.
login-page <url>	URL of the page that appears for the user logon. This can be set to any URL.

Parameter	Description
logon-wait	Configure parameters for the logon wait interval. 1-100 60
cpu-threshold <percent>	CPU utilization percentage above which the logon wait interval is applied when presenting the user with the logon page. 1-100 60
maximum-delay <seconds>	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. 1-10 10
minimum-delay <seconds>	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. 1-10 5
logout-popup-window	Enables a pop-up window with the Logout link that allows the user to log out. If this option is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads. enabled
max-authentication-failures <number>	Maximum number of authentication failures before the user is blacklisted/denylisted. 0-10 0
no	Negates any configured parameter.
protocol-http	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic. disabled
proxy	Update IP address of the proxy host.
redirect-pause <secs>	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link. 1-60 10
redirect-url <url>	URL to which an authenticated user will be directed. This parameter must be an absolute URL that begins with either http:// or https:// .

Parameter	Description
<code>server-group <group-name></code>	Name of the group of servers used to authenticate Captive Portal users.
<code>show-fqdn</code>	Allows the user to see and select the FQDN on the login page. The FQDNs shown are specified when configuring individual servers for the server group used with captive portal authentication. disabled
<code>single-session</code>	Allows only one active user session at a time. disabled
<code>show-acceptable-use-policy</code>	Show the acceptable use policy page before the login page. disabled
<code>switchip-in-redirectation-url</code>	Sends the IP address of the managed device in the redirection URL when external captive portal servers are used. An external captive portal server can determine the managed device from which a request originated by parsing the switchip variable in the URL. disabled
<code>url-hash-key <key></code>	Issue this command to hash the redirection URL using the specified key. disabled
<code>user-idle-timeout</code>	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-43200 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used. disabled
<code>user-logon</code>	Enables Captive Portal with authentication of user credentials. enabled
<code>user-vlan-in-redirectation-url</code>	Add the user VLAN in the redirection URL. disabled
<code>welcome-page <url></code>	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.
<code>white-list/allow-list</code>	Name of an existing whitelist/allowlist on an IPv4 or IPv6 network destination. The whitelist/allowlist contains authenticated websites that a guest can access. If you have not yet defined a netdestination, use the netdestination command to define a destination host or subnet before you add it to the whitelist/allowlist.

Example

The following example configures a Captive Portal authentication profile that authenticates users against the internal database. Users who are successfully authenticated are assigned the auth-guest role.

To create the auth-guest user role shown in this example, the PEFNG license must be installed in the Mobility Conductor.

```
(host)^[md] (config) #aaa authentication captive-portal guestnet
(host) ^[md] (Captive Portal Authentication Profile "guestnet") #default-role
auth-guest
(host) ^[md] (Captive Portal Authentication Profile "guestnet") #user-logon
(host) ^[md] (Captive Portal Authentication Profile "guestnet") #no guest-logon
(host) ^[md] (Captive Portal Authentication Profile "guestnet") #server-group
internal
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ All instances of <code>blacklist</code> have been replaced with <code>denylist</code>. ■ All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.7.0.0	Captive portal authentication was supported for VAPs in the bridge forwarding mode.
ArubaOS 8.4.0.0	The <code>ap-mac-in-redirectation-url</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on managed devices.

aaa authentication dot1x

```
aaa authentication dot1x {<profile>|countermeasures}
  ca-cert <certificate>
  cert-cn-lookup
  clear
  clone <profile>
  delete-keycache
  eapol-logoff
  enforce-suite-b-128
  enforce-suite-b-192
  framed-mtu <mtu>
  heldstate-bypass-counter <number>
  ignore-eap-id-match
  ignore-eapolstart-afterauthentication
  key-cache clear
  machine-authentication blacklist-on-failure / denylist-on-failure|{cache-timeout
  <hours>}|enable|
    {machine-default-role <role>}|{user-default-role <role>}
  max-authentication-failures <number>
  max-requests <number>
  multicast-keyrotation
  no ...
  opp-key-caching
  reauth-max <number>
  reauth-server-termination-action
  reauthentication
  reload-cert
  server {server-retry <number>|server-retry-period <seconds>}
  server-cert <certificate>
  termination {eap-type <type>}|enable|enable-token-caching|{inner-eap-type (eap-
  gtc|eap-mschapv2)}|{token-caching-period <hours>}
  timer {idrequest_period <seconds>}|{keycache-tmout <kc-tmout>}|{mkey-rotation-period
  <seconds>}|{quiet-period <seconds>}|{reauth-period <seconds>}|{ukey-rotation-period
  <seconds>}|{wpa_groupkey-delay <seconds>}|{wpa-key-period <milliseconds>}|wpa2-key-
  delay <milliseconds>
  tls-guest-access
  tls-guest-role <role>
  unicast-keyrotation
  use-session-key
  use-static-key
  validate-pmkid
  wep-key-retries <number>
  wep-key-size {40|128}
  wpa-fast-handover
  wpa-key-retries <number>
  xSec-mtu <mtu>
```

Description

This command configures the 802.1X authentication profile and allows you to enable and configure machine authentication and 802.1X termination on the managed device (also called AAA FastConnect). In the AAA profile, specify the 802.1X authentication profile, the default role for authenticated users, and the server group for the authentication.

Parameter	Description
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters. default
clear	Clear the Cached PMK, Role and VLAN entries. This command is available in enable mode only.
countermeasures	Scans for message integrity code failures in traffic received from clients. If there are more than 2 message integrity code failures within 60 seconds, the AP is shut down for 60 seconds. This option is intended to slow down an attacker who is making a large number of forgery attempts in a short time. disabled
ca-cert <certificate>	CA certificate for client authentication. The CA certificate needs to be loaded in the Mobility Conductor.
ca-cert-name	Name of the CA certificate.
cert-cn-lookup	If you use client certificates for user authentication, enable this option to verify that the CN of the certificate exists in the server. This parameter is disabled by default.
delete-keycache	Delete the key cache entry when the user entry is deleted. disabled
eapol-logoff	Enables handling of EAPOL-LOGOFF messages. disabled
enforce-suite-b-128	Configure Suite-B 128 bit or more security level authentication enforcement. disabled
enforce-suite-b-192	Configure Suite-B 192 bit or more security level authentication enforcement disabled
framed-mtu <MTU>	Sets the framed MTU attribute sent to the authentication server. 500-1500 1100

Parameter	Description
heldstate-bypass-counter <number>	This parameter is applicable when 802.1X authentication is terminated on the Mobility Conductor, also known as AAA FastConnect. Number of consecutive authentication failures which, when reached, causes the Mobility Conductor to not respond to authentication requests from a client while the Mobility Conductor is in a held state after the authentication failure. Until this number is reached, the Mobility Conductor responds to authentication requests from the client even while the Mobility Conductor is in its held state. 0-3 0
ignore-eap-id-match	Ignore EAP ID during negotiation. disabled
ignore-eapol-start-afterauthentication	Ignores EAPOL-START messages after authentication. disabled
key-cache clear	Clears the Cached PMK, Role and VLAN.
machine-authentication	This parameter is applicable in Windows environments only. These parameters set machine authentication. This parameter requires the PEFNG license.
blacklist-on-failure / denylist-on-failure	Blocks the client if machine authentication fails. disabled
cache-timeout <hours>	The timeout, in hours, for machine authentication. 1-1000 24
enable	Select this option to enforce machine authentication before user authentication. If selected, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful. disabled
machine-default-role <role>	Default role assigned to the user after completing only machine authentication. guest
user-default-role <role>	Default role assigned to the user after 802.1X authentication. guest

Parameter	Description
<code>max-authentication-failures <number></code>	<p>Number of times a user can try to login with wrong credentials after which the user is blocked as a security threat. Set to 0 to disable denylisting, otherwise enter a non-zero integer to block the user after the specified number of failures.</p> <p>0-5 0</p>
<code>max-requests <number></code>	<p>Maximum number of times ID requests are sent to the client.</p> <p>1-10 5</p>
<code>multicast-key rotation</code>	<p>Enables multicast key rotation</p> <p>disabled</p>
<code>no</code>	<p>Negates any configured parameter.</p>
<code>opp-key-caching</code>	<p>Enables a cached PMK derived with a client and an associated AP to be used when the client roams to a new AP. This allows clients faster roaming without a full 802.1X authentication. Make sure that the wireless client (the 802.1X supplicant) supports this feature. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the managed device can be out of sync with the key used by the client.</p> <p>enabled</p>
<code>reauth-max <number></code>	<p>Maximum number of reauthentication attempts.</p> <p>1-10 3</p>
<code>reauth-server-termination-action</code>	<p>Specifies the termination-action attribute from the server.</p>
<code>reauthentication</code>	<p>Select this option to force the client to do a 802.1X reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.) If the user fails to reauthenticate with valid credentials, the state of the user is cleared.</p> <p>If derivation rules are used to classify 802.1X-authenticated users, then the reauthentication timer per role overrides this setting.</p> <p>disabled</p>
<code>reload-cert</code>	<p>Reload certificate for 802.1X termination. This command is available in enable mode only.</p>

Parameter	Description
server	Sets options for sending authentication requests to the authentication server group.
server-retry <number>	Maximum number of authentication requests that are sent to server group. 0-5 3
server-retry-period <seconds>	Server group retry interval, in seconds. 2-65535 5
server-cert <certificate>	Server certificate used by the managed device to authenticate itself to the client.
termination	Sets options for terminating 802.1X authentication on the managed device.
eap-type <type>	The EAP method, either EAP-PEAP or EAP-TLS. eap-peap, eap-tls eap-peap
enable	Enables 802.1X termination on the managed device. disabled
enable-token -caching	If you select EAP-GTC as the inner EAP method, you can enable the Mobility Conductor to cache the username and password of each authenticated user. The Mobility Conductor continues to reauthenticate users with the remote authentication server, however, if the authentication server is not available, the Mobility Conductor will inspect its cached credentials to reauthenticate users. disabled
inner-eap-type eap-gtc eap-mschapv2	When EAP-PEAP is the EAP method, one of the following inner EAP types is used: EAP-GTC: Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Mobility Conductor as a backup to an external authentication server. EAP-MSCHAPv2: Described in RFC 2759, this EAP method is widely supported by Microsoft clients. eap-gtc, eap- mschapv2 eap-mschapv2

Parameter	Description
token-caching-period <hours>	If you select EAP-GTC as the inner EAP method, you can specify the timeout period, in hours, for the cached information. 24
timer	Sets timer options for 802.1X authentication:
idrequest-period <seconds>	Interval, in seconds, between identity request retries. 1-65535 5
keycache-tmout	Set the per BSSID PMKSA cache interval. Cache is deleted within 2 hours of the interval. 1-2000 8
mkey-rotation-period <seconds>	Interval, in seconds, between multicast key rotation. 60-864000 1800
quiet-period <seconds>	Interval, in seconds, following failed authentication. 1-65535 30
reauth-period <seconds>	Interval, in seconds, between reauthentication attempts, or specify server to use the server-provided reauthentication period. 60-864000 86400
ukey-rotation-period <seconds>	Interval, in seconds, between unicast key rotation. 60-86400 900
wpa-groupkey-delay <milliseconds>	Interval, in milliseconds, between unicast and multicast key exchanges. 0-2000 0
wpa-key-period <milliseconds>	Interval, in milliseconds, between each WPA key exchange. 10-5000 1000
wpa2-key-delay <milliseconds>	Set the delay between EAP-Success and unicast key exchange.

Parameter	Description
	1-2000 0
<code>tls-guest-access</code>	Enables guest access for EAP-TLS users with valid certificates. disabled
<code>tls-guest-role <role></code>	User role assigned to EAP-TLS guest. This parameter requires the PEFNG license. guest
<code>unicast-keyrotation</code>	Enables unicast key rotation. disabled
<code>use-session-key</code>	Use RADIUS session key as the unicast WEP key. disabled
<code>use-static-key</code>	Use static key as the unicast or multicast WEP key. disabled
<code>validate-pmkid</code>	This parameter instructs the Mobility Conductor to check the PMK ID sent by the client. When this option is enabled, the client must send a PMK ID in the associate or reassociate frame to indicate that it supports OKC or PMK caching; otherwise, full 802.1X authentication takes place. (This feature is optional, since most clients that support OKC and PMK caching do not send the PMKID in their association request.) disabled
<code>wep-key-retries <number></code>	Number of times WPA or WPA2 key messages are retried. 1-3 2
<code>wep-key-size</code>	Dynamic WEP key size, either 40 or 128 bits. 128
<code>wpa-fast-handover</code>	Enables WPA-fast-handover. This is only applicable for phones that support WPA and fast handover. disabled
<code>wpa-key-retries</code>	Set the number of times WPA or WPA2 Key Messages are retried. The supported range is 1-10 retries, and the default value is 3.
<code>xSec-mtu <mtu></code>	Sets the size of the MTU for xSec. 1024-1500 1300

Examples

The following example enables authentication of the user's client device before user authentication. If machine authentication fails but user authentication succeeds, the user is assigned the restricted guest role:

```
(host) ^[md] (config) #aaa authentication dot1x dot1x
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication enable
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication
machine-default-role computer
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication user-
default-role guest
```

The following example configures an 802.1X profile that terminates authentication on the managed device, where the user authentication is performed with the internal database of the managed device or to a "backend" non-802.1X server:

```
(host) ^[md] (config) #aaa authentication dot1x dot1x
(host) ^[md] (802.1X Authentication Profile "dot1x") #termination enable
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system. The voice-aware parameter requires the PEFNG license.	Config mode on Mobility Conductor.

aaa authentication mac

```
aaa authentication mac <profile>
  case upper|lower
  clone <profile>
  delimiter {colon|dash|none}
  max-authentication-failures <number>
  no ...
  reauthentication
  timer reauth period {<ra-period>|server}
```

Description

This command configures the MAC authentication profile, which configures authentication of devices based on their physical MAC address. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to all other devices. Users may be required to authenticate themselves using other methods, depending on the network privileges.

Parameter	Description
<profile>	Name that identifies an instance of the profile. The name must be 1-63 characters.
case	The case (upper or lower) used in the MAC string sent in the authentication request. If there is no delimiter configured, the MAC address in lower case is sent in the format xxxxxxxxxxxx, while the MAC address in upper case is sent in the format XXXXXXXXXXXX. upper, lower lower
clone <profile>	Name of an existing MAC profile from which parameter values are copied.
delimiter	Delimiter (colon, dash, none, oui-nic) used in the MAC string. colon, dash, none, oui-nic none
max-authentication-failures <number>	Number of times a client can fail to authenticate before it is blocked. A value of 0 disables blacklisting/denylisting. 0-10 0
no	Negates any configured parameter.
reauthentication	Use this parameter to enable or disable reauthentication. disabled
timer reauth period <ra-period> server	<ra-period> specifies the period between reauthentication attempts in seconds. The server parameter specifies the server-provided reauthentication interval. 60-86400 86400

Example

The following example configures a MAC authentication profile to block client devices that fail to authenticate.

```
(host) ^[md] (config) #aaa authentication mac mac-denylist
(host) ^[md] (MAC Authentication Profile "mac-denylist") #max-authentication-
failures 3
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication mgmt

```
aaa authentication mgmt
  default-role {ap-provisioning|guest-provisioning|location-api-mgmt|nbapi-mgmt|network-
  operations|no-access|read-only|root|standard}
  enable
  mchapv2
  no ...
  server-group <group>
```

Description

This command configures authentication for administrative users. If you enable authentication with this command, users configured with the `mgmt-user` command must be authenticated using the specified `server-group`.

You can configure the management authentication profile in the base operating system or with the PEFNG license installed.

Syntax

Parameter	Description
<code>default-role</code>	Select a predefined management role to assign to authenticated administrative users:
<code>ap-provisioning</code>	AP provisioning role.
<code>guest-provisioning</code>	Guest provisioning role.
<code>location-api-mgmt</code>	Location API management role.
<code>nbapi-mgmt</code>	NBAPI management role.
<code>network-operations</code>	Network operator role.
<code>read-only</code>	Read-only role.
<code>root</code>	Default role or superuser role.
<code>standard</code>	Standard role
<code>enable</code>	Enables authentication for administrative users. disabled
<code>mchapv2</code>	Enable MSCHAPv2. disabled
<code>no</code>	Negates any configured parameter.
<code>server-group <group></code>	Name of the group of servers used to authenticate administrative users.

Example

The following example configures a management authentication profile that authenticates users against the internal database of the Mobility Conductor. Users who are successfully authenticated are assigned the read-only role.

```
(host) [mynode] (config) aaa authentication mgmt
default-role read-only
server-group internal
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The standard parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication-server internal

```
aaa authentication-server internal
  use-local-switch
```

Description

This command specifies that the internal database on a managed device must be used for authenticating clients.

Parameter	Description
use-local-switch	Use the internal database on the local managed device. By default, the internal database on the Mobility Conductor is used for authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor executed on the managed device node.

aaa auth-survivability

```
aaa auth-survivability
  cache-lifetime
  enable
  server-cert
```

Description

This command configures authentication survivability on a managed device.

Parameter	Description
cache-lifetime <hrs>	<p>This parameter specifies the lifetime in hours for the cached access credential in the local Survival Server. When the specified cache-lifetime expires, the cached access credential is deleted from the managed device.</p> <p>1-72 1</p>
enable	<p>This parameter controls whether to use the Survival Server when no other servers in the server group are in-service. This parameter also controls whether to store the user access credential in the Survival Server when it is authenticated by an external RADIUS or LDAP server in the server group. Authentication Survivability is enabled or disabled on each managed device. Authentication survivability will not activate if the Authentication Server Dead Time is configured as 0</p> <p>Disabled</p>
server-cert	<p>This parameter allows you to view the name of the server certificate used by the local Survival Server. The local Survival Server is provided with a default server certificate from AOS. The customer server certificate must be imported into the managed device first, and then you can assign the server certificate to the local Survival Server.</p> <p>NOTE: In the deployment environment, it is recommended that you switch to a customer server certificate.</p>

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication-server ldap

```
aaa authentication-server ldap <server>
  admin-dn <name>
  admin-passwd <string>
  allow-clear-text
  authport <port>
  base-dn <name>
  chase-referrals
  clone <server>
  enable
  filter <filter>
  host <ipaddr>
  key-attribute <string>
  max-connection <number>
  no ...
  preferred-conn-type ldap-s|start-tls|clear-text
  timeout <seconds>
```

Description

This command configures an LDAP server. You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see [aaa server-group on page 103](#)).



A maximum of 128 LDAP servers can be configured on the Mobility Conductor.

Parameter	Description
<server>	Name that identifies the server.
admin-dn <name>	DN for the admin user who has read or search privileges across all of the entries in the LDAP database (the user does not need write privileges but should be able to search the database and read attributes of other users in the database).
admin-passwd <string>	Password for the admin user.
allow-clear-text	Allows clear-text (unencrypted) communication with the LDAP server. Disabled
authport <port>	Port number used for authentication. Port 636 will be attempted for LDAP over SSL-LDAP, while port 389 will be attempted for SSL over LDAP, Start TLS operation and clear text. 1-65535 389
base-dn <name>	DN name of the node which contains the entire user database to use.
chase-referrals	Chase referrals anonymously.

Parameter	Description
<code>clone <server></code>	Name of an existing LDAP server configuration from which parameter values are copied.
<code>enable</code>	Enables the LDAP server.
<code>filter <filter></code>	Filter that should be applied to search of the user in the LDAP database. (objectclass=*)
<code>host <ip-addr></code>	IP address of the LDAP server, in dotted-decimal format.
<code>key-attribute <string></code>	Attribute that should be used as a key in search for the LDAP server. For PAP, the value is sAMAccountName. For EAP-TLS termination the value is userPrincipalName. sAMAccountName
<code>max-connection</code>	Maximum number of simultaneous non-admin connections to an LDAP server.
<code>no</code>	Negates any configured parameter.
<code>preferred-conn-type</code>	Preferred connection type. The default order of connection type is: 1. ldap-s 2. start-tls 3. clear-text The Mobility Conductor will first try to contact the LDAP server using the preferred connection type, and will only attempt to use a lower-priority connection type if the first attempt is not successful. You enable the allow-cleartext option before you select clear-text as the preferred connection type. If you set clear-text as the preferred connection type but do not allow clear-text, the Mobility Conductor will only use ldap-s or start-tls to contact the LDAP server. ldap-s, start-tls, clear-text ldap-s
<code>timeout <seconds></code>	Timeout period of a LDAP request, in seconds. 1-30 20

Example

The following command configures and enables an LDAP server:

```
(host) ^[md] (config) #aaa authentication-server ldap ldap1
(host) ^[md] (LDAP Server "ldap1") #host 10.1.1.243
(host) ^[md] (LDAP Server "ldap1") #base-dn cn=Users,dc=lm,dc=corp,dc=com
(host) ^[md] (LDAP Server "ldap1") #admin-dn cn=corp,cn=Users,dc=lm,dc=corp,dc=com
(host) ^[md] (LDAP Server "ldap1") #admin-passwd abc10
(host) ^[md] (LDAP Server "ldap1") #key-attribute sAMAccountName
(host) ^[md] (LDAP Server "ldap1") #filter (objectclass=*)
(host) ^[md] (LDAP Server "ldap1") #enable
```


Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication-server radius

```
aaa authentication-server radius <rad_server_name>
  acct-modifier <profile_name>
  acctport <port>
  authport <port>
  auth-modifier <profile_name>
  called-station-id type
    {ap-group | ap-macaddr | ap-name | ipaddr | macaddr | vlan-id}
    [delimiter {colon | dash | none}] [include-ssid {enable |disable}]
  clone <server>
  cppm username <username> password <password>
  enable
  enable-ipv6
  enable-radsec
  host <ipaddr>|<FQDN>
  key <psk>
  mac-delimiter [colon | dash | none | oui-nic]
  mac-lowercase
  nas-identifier <string>
  nas-ip <ipaddr>
  nas-ip6 <ipv6-address>
  no
  radsec-client-cert-name <name>
  radsec-port <radsec-port>
  radsec-trusted-cacert-name <radsec-trusted-ca>
  radsec-trusted-servercert-name <name>
  retransmit <number>
  service-type-framed-user
  source-interface vlan <vlan> ip6addr <ipv6addr>
  timeout <seconds>
  use-ip-for-calling-station
  use-md5
```

Description

This command configures a RADIUS server. You can configure a server before you can add it to one or more server groups. You can create a server group for a specific type of authentication (see [aaa server-group on page 103](#)).

Parameter	Description
<rad_server_name>	Name that identifies the server.
acct-modifier <profile_name>	Attributes modifier for accounting-request.
acctport <port>	Accounting port on the server. 1-65535 1813
authport <port>	Authentication port on the server. 1-65535 1812

Parameter	Description
<code>auth-modifier</code>	Attributes modifier for access-request.
<code>called-station-id type</code> { <code>ap-group</code> <code>ap-macaddr</code> <code>ap-name</code> <code>ipaddr</code> <code>macaddr</code> <code>vlan-id</code> }	Configure this parameter to be sent with the RADIUS attribute Called Station ID for authentication and accounting requests. The <code>called-station-id</code> parameter can be configured to include AP group, AP MAC address, AP name, Mobility Conductor IP, Mobility Conductor MAC address, or user vlan. The default value is Mobility Conductor MAC address. <code>macaddr</code>
<code>clone <server></code>	Name of an existing RADIUS server configuration from which parameter values are copied.
<code>c ppm username <username></code> <code>password <password></code>	Configure the ClearPass Policy Manager username and password. The Mobility Conductor authenticating to ClearPass Policy Manager is enhanced to use configurable username and password instead of support password. The support password is vulnerable to attacks as the server certificate presented by ClearPass Policy Manager server is not validated.
<code>enable</code>	Enables the RADIUS server.
<code>enable-ipv6</code>	Enables the RADIUS server in IPv6 mode.
<code>enable-radsec</code>	Enables RadSec for RADIUS data transport over TCP and TLS.
<code>host</code>	Identify the RADIUS server either by its IP address or FQDN.
<code><ipaddr></code>	IPv4 or IPv6 address of the RADIUS server.
<code><FQDN></code>	FQDN of the RADIUS server. The maximum supported length is 63 characters.
<code>key <psk></code>	Shared secret between the Mobility Conductor and the authentication server. The maximum length is 128 characters.
<code>mac-delimiter</code> [<code>colon</code> <code>dash</code> <code>none</code> <code>oui-nic</code>]	Send MAC address with user-defined delimiter. <code>none</code>
<code>mac-lowercase</code>	Send MAC addresses as lowercase.
<code>nas-identifier <string></code>	NAS identifier to use in RADIUS packets.
<code>nas-ip <ip-addr></code>	The NAS IP address to be sent in RADIUS packets from that server. If you define a local NAS IP setting using this command and also define a global NAS IP using the command <code>ip radius nas-ip <ip-addr></code> , the global NAS IP address takes precedence.
<code>nas-ip6 <ipv6-address></code>	NAS IPv6 address to send in RADIUS packets. You can configure a global NAS IPv6 address that the Mobility Conductor uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IPv6, the global NAS IPv6 is used. To set the global NAS IPv6, enter the <code>ipv6 radius nas-ip6 <ipv6-address></code> command.

Parameter	Description
no	Negates any configured parameter.
radsec-client-cert <radsec-client-cert>	Configures a RadSec client certificate on the RADIUS server to identify and authenticate clients.
radsec-port <radsec-port>	Designates a RadSec port for RADIUS data transport. 1-65535 2083
radsec-trusted-cacert-name <radsec-trusted-ca>	Designates a CA to sign RadSec certificates.
radsec-trusted-servercert-name <radsec-trusted-ca>	Designates a trusted RadSec server certificate.
retransmit <number>	Maximum number of retries sent to the server by the Mobility Conductor before the server is marked as down. 0-3 3
service-type-framed-user	Send the service-type as FRAMED-USER instead of LOGIN-USER. This option is disabled by default. disabled
source-interface vlan <vlan> ip6addr <ip6addr>	This option associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. <ul style="list-style-type: none"> ■ If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address. ■ If you do not associate the Source Interface with a configured server (leave the field blank), then the IP address of the global Source Interface will be used. ■ If you want to configure an IPv6 address for the Source Interface, specify the IPv6 address for the <code>ip6addr</code> parameter.
timeout <seconds>	Maximum time, in seconds, that the Mobility Conductor waits before timing out the request and resending it. 1-30 5 Starting from ArubaOS 8.10.0.0, the range of the RADIUS server authentication timeout value is increased from 1-30 seconds to 1-120 seconds.
use-ip-for-calling-station	Use an IP address instead of a MAC address for calling station IDs. This option is disabled by default. disabled
use-md5	Use MD5 hash of cleartext password. disabled

Example

The following command configures and enables a RADIUS server:

```
(host) [md] (config) #aaa authentication-server radius radius
(host) [md] (RADIUS Server "radius") #host 10.1.1.244
(host) [md] (RADIUS Server "radius") #key qwERTyuIop
(host) [md] (RADIUS Server "radius") #enable
```

Command History

Release	Modification
ArubaOS 8.10.0.0	The range of the RADIUS server authentication timeout value was increased from 1-30 seconds to 1-120 seconds.
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none">■ acct-modifier■ auth-modifier
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication-server tacacs

```
aaa authentication-server tacacs <server>
  clone <source>
  enable
  host <host>
  key <psk>
  no ...
  retransmit <number>
  session-authorization
  source-interface
  tcp-port <port>
  timeout <seconds>
```

Description

This command configures a TACACS+ server. You can configure a server before you can add it to one or more server groups. You can create a server group for a specific type of authentication (see [aaa server-group on page 103](#)).

A maximum of 128 TACACS servers can be configured on the Mobility Conductor.

Parameter	Description
<server>	Name that identifies the server.
clone <source>	Name of an existing TACACS server configuration from which parameter values are copied.
enable	Enables the TACACS server.
host <host>	IPv4 or IPv6 address of the TACACS server.
key	Shared secret to authenticate communication between the TACACS client and server.
no	Negates any configured parameter.
retransmit <number>	Maximum number of times a request is retried. 0-3 3
session-authorization	Enables TACACS+ authorization. Session-authorization turns on the optional authorization session for admin users. disabled
source-interface	Select source address of outgoing TACACS requests to the server.
vlan <vlan_id>	Select VLAN of outgoing TACACS requests to the server. 1-4094
tcp-port <port>	TCP port used by the server. 1-65535 49

Parameter	Description
timeout <timeout>	Timeout period of a TACACS request, in seconds. 1-30 20

Example

The following command configures, enables a TACACS+ server and enables session authorization:

```
(host) ^[md] (config) #aaa authentication-server tacacs tacacs1
(host) ^[md] (TACACS Server "tacacs1")clone default
(host) ^[md] (TACACS Server "tacacs1")host 10.1.1.245
(host) ^[md] (TACACS Server "tacacs1")key qwERtyuIOp
(host) ^[md] (TACACS Server "tacacs1")enable
(host) ^[md] (TACACS Server "tacacs1")session-authorization
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>source-interface</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor

aaa authentication-server windows

```
aaa authentication-server windows <windows_server_name>
  clone <source>
  domain <domain>
  enable
  host <ipaddr>
  no
```

Description

This command configures a windows server for stateful-NTLM authentication. You must define a Windows server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see [aaa server-group on page 103](#)). Windows servers are used for stateful-NTLM authentication.

Parameter	Description
<windows_server_name>	Name of the windows server. You will use this name when you add the windows server to a server group.
clone <source>	Name of a Windows Server from which you want to make a copy.
domain <domain>	The Windows domain for the authentication server.
enable	Enables the Windows server.
host <ipaddr>	IP address of the Windows server.
no	Delete command.

Example

The following command configures and enables a windows server:

```
(host) ^[md] (config) #aaa authentication-server windows IAS_1
(host) ^[md] (Windows Server "IAS_1") #host 10.1.1.245
(host) ^[md] (Windows Server "IAS_1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication stateful-dot1x

```
aaa authentication stateful-dot1x
  default-role <role>
  enable
  no ...
  server-group <group>
  timeout <seconds>
```

Description

This command configures 802.1X authentication for clients on non-Aruba APs. This command configures 802.1X authentication for clients on non-Aruba APs. The Mobility Conductor maintains user session state information for these clients.

Parameter	Description
default-role <role>	Role assigned to the 802.1X user upon login. The PEFNG license must be installed. guest
enable	Enables 802.1X authentication for clients on non-Aruba APs. Use <code>no enable</code> to disable stateful 802.1X authentication. enabled
no	Negates any configured parameter.
server-group <group>	Name of the group of RADIUS servers used to authenticate the 802.1X users.
timeout <seconds>	Timeout period, in seconds. 1-20 10

Example

The following command assigns the employee user role to clients who successfully authenticate with the server group corp-rad:

```
(host) ^[md] (config) aaa authentication stateful-dot1x
default-role employee
server-group corp-rad
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication stateful-dot1x clear

aaa authentication stateful-dot1x clear

Description

This command clears automatically-created control path entries for 802.1X users on non-Aruba APs. Run this command after changing the configuration of a RADIUS server in the server group configured with the `aaa authentication stateful-dot1x` command. This causes entries for the users to be created in the control path with the updated configuration information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor in the managed device node.

aaa authentication stateful-kerberos

```
aaa authentication stateful-kerberos <profile-name>
  clone
  default-role <role>
  no
  server-group <server-group>
  timeout <timeout>
```

Description

This command configures stateful Kerberos authentication.

Parameter	Description
clone <source>	Create a copy of an existing stateful Kerberos profile
default-role	Select an existing role to assign to authenticated users. guest
no	Negates any configured parameter.
server-group <server-group>	Name of a server group. default
timeout <timeout>	Amount of time, in seconds, before the request times out. 1-20 seconds 10 seconds

Example

```
(host) ^[md] (config) #aaa authentication stateful-kerberos default
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #default-role
guest
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #timeout 10
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #server-group
internal
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication stateful-ntlm

```
aaa authentication stateful-ntlm <profile-name>
  clone
  default-role <role>
  enable
  no
  server-group <server-group>
  timeout <timeout>
```

Description

NTLM is a suite of Microsoft authentication and session security protocols. You can use a stateful NTLM authentication profile to configure a managed device to monitor the NTLM authentication messages between clients and an authentication server. The managed device can then use the information in the SMB headers to determine the username and IP address of the client, the server IP address and the current authentication status client. If the client successfully authenticates via an NTLM authentication server, the managed device can recognize that the client has been authenticated and assign that client a specified user role. When the user logs off or shuts down the client machine, the user will remain in the authenticated role until the user's authentication is aged out.

The stateful NTLM Authentication profile requires that you specify a server group which includes the servers performing NTLM authentication, and a default role to be assigned to authenticated users. For details on defining a windows server used for NTLM authentication, see [aaa authentication-server windows](#).

Parameter	Description
clone	Create a copy of an existing stateful NTLM profile
default-role	Select an existing role to assign to authenticated users. guest
enable	Enables stateful ntlm authentication profile for clients. Use <code>no enable</code> to disable stateful ntlm authentication. enabled
no	Negates any configured parameter.
server-group <server-group>	Name of a server group. default
timeout <timeout>	Amount of time, in seconds, before the request times out. 1-20 seconds 10 seconds

Example

The following example configures a stateful NTLM authentication profile that authenticates clients via the server group "Windows1." Users who are successfully authenticated are assigned the "guest2" role.

```
(host) ^[md] (config) #aaa authentication stateful-ntlm ntlm1
(host) ^[md] (Stateful NTLM Authentication Profile "ntlm1") #default-role guest2
(host) ^[md] (Stateful NTLM Authentication Profile "ntlm1") #server-group Windows1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa auth-trace

```
aaa auth-trace
  loglevel
```

Description

This command sets parameters for debug tracing in AUTH (light weight tracing).

Parameter	Description
loglevel	Specify the loglevel of syslogs that will be included in the trace.
alert	Trace all logs equal or higher than LOG_ALERT.
critical	Trace all logs equal or higher than LOG_CRIT.
debug	Trace all logs equal or higher than LOG_DEBUG.
emergency	Trace all logs equal or higher than LOG_EMERG.
error	Trace all logs equal or higher than LOG_ERR.
info	Trace all logs equal or higher than LOG_INFO.
notice	Trace all logs equal or higher than LOG_NOTICE.
warn	Trace all logs equal or higher than LOG_WARN.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor in the managed device node.

aaa authentication via auth-profile

```
aaa authentication via auth-profile <profile>
  auth-protocol {mschapv2|pap}
  cert-cn-lookup
  client-cert-enable
  clone <source>
  default-role <default-role>
  desc <description>
  download-role
  encoding-format
  max-authentication-failures <max-authentication-failures>
  no
  pan-integration
  radius-accounting <server_group_name>
  rfc-3576-server <rfc-server>
  server-group <server-group>
```

Description

This command configures the VIA authentication profile and associates user roles to the authentication profile.

Parameter	Description
auth-protocol {mschapv2 pap}	Authentication protocol support for VIA authentication; MSCHAPv2 or PAP PAP
cert-cn-lookup	Check certificate CN against AAA server. Enabled
client-cert-enable	If selected, this option enables client certificate-based authentication for VPN profile download. Disabled
clone <source>	Name of an existing profile from which configuration values are copied.
default-role <default-role>	Name of the default VIA authentication profile.
desc <description>	Description of this profile for reference.
download-role	Name of the authentication profile to be downloaded from CPPM.
encoding-format	Specify one of the following encoding format type for the user credentials: <ul style="list-style-type: none">■ ANSI■ UTF-16■ UTF-8 The default type is UTF-8.

Parameter	Description
max-authentication-failures <max-authentication-failures>	Number of times VIA will prompt user to login due to incorrect credentials. After the maximum authentication attempts failures VIA will exit. 0
pan-integration	Requires IP mapping at Palo Alto Network.
radius-accounting <server_group_name>	Server group for RADIUS accounting.
rfc-3576-server <rfc-server>	Configures the RFC 3576 server.
server-group <server-group>	Server group against which the user is authenticated.

Example

```
(host) [md] (config) #aaa authentication via auth-profile default
(host) [md] (VIA Authentication Profile "default") #auth-protocol mschapv2
(host) [md] (VIA Authentication Profile "default") #default-role example-via-role
(host) [md] (VIA Authentication Profile "default") #desc "Default VIA
Authentication Profile"
(host) [md] (VIA Authentication Profile "default") #server-group "via-server-
group"
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication via connection-profile

```
aaa authentication via connection-profile <profile>
  admin-logout-script
  admin-logon-script
  allow-user-disconnect
  allow-whitelist-traffic / allow-allowlist-traffic
  auth-profile
  auth_domain_suffix
  auto-launch-supPLICANT
  auto-login
  auto-upgrade
  banner-message-reappear-timeout <mins>
  block-dest-traffic
  block-destination-traffic-selector
  certificate-criteria
  client-logging
  client-netmask
  client-wlan-profile <client-wlan-profile> position <position>
  clone <source>
  controllers-load-balance
  csec-gateway-url <URL>
  csec-http-ports <comma separated port numbers>
  dn-profile
  dns-suffix-list <dns-suffix-list>
  domain-pre-connect
  DPC-generate-profile
  enable-csec
  enable-fips
  enable-supPLICANT
  ext-download-url <ext-download-url>
  ike-policy <ike-policy>
  ikev2-policy
  ikev2-proto
  ikev2auth
  ipsec-cryptomap map <map> number <number>
  ipsecv2-cryptomap
  l2-forwarding
  lockdown-all-settings
  max-reconnect-attempts <max-reconnect-attempts>
  max-timeout <value>
  minimized
  mtu
  no
  oosp-responder
  save-passwords
  server
  split-tunneling
  suiteb-crypto
  support-email
  tos-dscp {0-63}
  tunnel
  user-idle-timeout
  validate-server-cert
  via_cc_log_enable
  whitelist/allowlist
  windows-credentials
```

Description

This command configures the VIA connection profile. A VIA connection profile contains settings required by VIA to establish a secure connection to the managed device. You can configure multiple VIA connection profiles. A VIA connection profile is always associated to a user role and all users belonging to that role will use the configured settings. If you do not assign a VIA connection profile to a user role, the default connection profile is used.

Parameter	Description
<code>admin-logoff-script</code>	Enables VIA logoff script. Disabled
<code>admin-logon-script</code>	Enables VIA logon script. Disabled
<code>allow-user-disconnect</code>	Enable or disable users to disconnect their VIA sessions. Enabled
<code>allow-whitelist-traffic / allow-allowlist-traffic</code>	If enabled, this feature will block network access until the VIA VPN connection is established. Disabled
<code>auth-profile <auth-profile></code>	This is the list of VIA authentication profiles that will be displayed to users in the VIA client.
<code>auth_domain_suffix</code>	Enables a domain suffix on VIA Authentication, so client credentials are sent as <i>domainname\username</i> instead of just <i>username</i> .
<code>auto-launch-supPLICANT</code>	Allows you to connect automatically to a configured WLAN network. Disabled
<code>auto-login</code>	Enable or disable VIA client to auto login and establish a secure connection to the managed device. Enabled
<code>auto-upgrade</code>	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the managed device. Enabled
<code>banner-message-reappear- timeout</code>	Timeout value, in minutes, after which the user session will end and the VIA Login banner message reappears. 1440
<code>block-destination-traffic- selector-ON</code>	Turn ON feature to block Destination Traffic .
<code>block-dest-traffic-address</code>	Destination Traffic selector.
<code>certificate-criteria</code>	Allows admin users to filter the certificates that can be used to establish the IPsec connection when a user certificate or EAP-TLS is used as the authentication method. Use the following certificate attributes or OIDs to set the certificate criteria:

Parameter	Description
	<ul style="list-style-type: none"> ■ commonName (OID 2.5.4.3) ■ organizationalUnitName (OID 2.5.4.11) ■ organizationName (OID 2.5.4.10) ■ subjectAltName (OID 2.5.29.17) ■ certificateIssuer (OID 2.5.29.29) ■ userPrincipalName (OID 1.3.6.1.4.1.311.20.2.3) ■ emailAddress (OID 1.2.840.113549.1.9.1) ■ friendlyName (OID 1.2.840.113549.1.9.20) <p>The maximum length is 256 characters. Each attribute or OID must be separated by a semicolon. If an attribute or OID contains any spaces, the entire string must be enclosed in quotation marks.</p>
client-logging	<p>Enable or disable VIA client to auto login and establish a secure connection to the managed device.</p> <p>Enabled</p>
client-netmask <client-netmask>	<p>The network mask that has to be set on the client after the VPN connection is established.</p> <p>255.255.255.255</p>
client-wlan-profile <client-wlan-profile>	<p>A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config to configure or manage their wireless networks.</p>
clone <source>	<p>Create a copy of connection profile from an another VIA connection profile.</p>
controllers-load-balance	<p>Enable this option to allow the VIA client to failover to the next available selected randomly from the list as configured in the VIA Servers option. If disabled, VIA will failover to the next in the sequence of ordered list of VIA servers.</p> <p>Disabled</p>
csec-gateway-url	<p>Specify the content security service providers URL here. You must provide a FQDN.</p>
csec-http-ports	<p>Specify the ports (separated by comma) that will be monitored by the content security service provider. Do not add space before or after the comma.</p>
dn-profile CN ORG OU Country	<p>Configure VIA dn profile.</p> <p>NOTE: If a hyphen is entered as an input after a parameter, the controller and VIA will then ignore that parameter. The following example ignores the OU parameter,</p> <pre>(host) [md] (config) #aaa authentication via connection-profile "via" (host) [md] (VIA Connection Profile "via") #dn-profile CN VIA-EXAMPLE.ACME.COM ORG IT OU - Country USA</pre>
dns-suffix-list <dns-suffix-list>	<p>The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established.</p> <p>None</p>

Parameter	Description
<code>domain-preconnect</code>	Enable this option to allow users with lost or expired passwords to establish a VIA connection to corporate network. This option authenticates the user's device and establishes a VIA connection that allows users to reset credentials and continue with corporate access. Enabled
<code>dpc-generate-profile</code>	Optionally enable generating common profile in DPC is enabled.
<code>enable-csec</code>	Use this option to enable the content security service.
<code>enable-fips</code>	Enable the VIA FIPS module so VIA checks for FIPS compliance during startup. Disabled
<code>enable-supPLICant</code>	If enabled, VIA starts in bSec mode using L2 suite-b cryptography. This option is disabled by default. Disabled
<code>ext-download-url <ext-download-url></code>	End users will use this URL to download VIA on their computers.
<code>ike-policy <ike-policy></code>	List of IKE policies that the VIA Client has to use to connect to the managed device.
<code>ikev2-policy</code>	List of IKE V2 policies that the VIA Client has to use to connect to the managed device.
<code>ikev2-PROTO</code>	Enable this to use IKEv2 protocol to establish VIA sessions. Disabled
<code>ikev2auth</code>	Use this option to set the IKEv2 authentication method. By default user certificate is used for authentication. The other supported methods are EAP-MSCHAPv2, EAP-TLS. The EAP authentication is done on an external RADIUS server. User Certificates
<code>ipsec-cryptomap</code>	List of IPsec crypto maps that the VIA client uses to connect to the managed device. These IPsec Crypto Maps are configured in the CLI using the <code>crypto-local ipsec-map <ipsec-map-name></code> command.
<code>ipsecv2-cryptomap</code>	List of IPsec V2 crypto maps that the VIA client uses to connect to the managed device.
<code>l2-forwarding</code>	Enable this option to forward Layer-2 GRE tunnel.
<code>lockdown-all-settings</code>	Allows you to lock down all user-configured settings. Disabled
<code>max-reconnect-attempts <max-reconnect-attempts></code>	The maximum number of re-connection attempts by the VIA client due to authentication failures. 3
<code>max-timeout value <value></code>	The maximum time (minutes) allowed before the VIA session is disconnected.

Parameter	Description
	1440
minimized	Use this option to keep the VIA client on a Microsoft Windows operating system minimized to system tray.
mtu	MTU value in bytes for the VIA client. 576-5120 1452
ocsp-responder	OCSP Cert Verification.
enable	Enable or disable OCSP Cert verification.
fallback	Action taken when OCSP Cert verification result is unknown.
save-passwords	Enable or disable users to save passwords entered in VIA. Enabled
server	Configure VIA servers.
addr <addr>	This is the public IPv4 or IPv6 address or the DNS hostname of the managed device connected to VIA. Users connect to remote server using this IP address or the host name.
<internal-ip <internal-ip>	This is the IPv4 address of any of the VLAN interface IPv4 addresses that belongs to this managed device.
desc <description>	This is a human-readable description of the managed device.
split-tunneling	Enable or disable split tunneling. <ul style="list-style-type: none"> ■ If enabled, all traffic to the VIA tunneled networks will go through the managed device and the rest is just bridged directly on the client. ■ If disabled, all traffic will flow through the managed device. Off
suiteb-crypto	Use this option to enable Suite-B cryptography. See RFC 4869 for more information about Suite-B cryptography. Disabled
support-email	The support e-mail address to which VIA users will send client logs. None
tos-dscp {0-63}	Use this to mark IPsec packets with higher QoS/DSCP than Best Effort. The range is 0-63. 0
tunnel address <address>	A list of network destination (IP address and netmask) that the VIA client will tunnel through the managed device. All other network destinations will be reachable directly by the VIA client. Enter tunneled IP address and its netmask.
address <address>	
netmask <netmask>	

Parameter	Description
user-idle-timeout	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used. Disabled
validate-server-cert	Enable or disable VIA from validating the server certificate presented by the managed device. Enabled
vis_cc_log_enable	Enable VIA CC compliance packet level logging.
whitelist addr /allowlist addr	Specify a hostname or IP address and network mask to define a whitelist/allowlist of users allowed to access the network if the allow-whitelist-traffic / allow-allowlist-traffic option is enabled. The maximum number of entries allowed is 16.
addr <addr>	Host name of IP address of a client
netmask <netmask>	Netmask, in dotted decimal format
description <description>	(Optional) description of the client
windows-credentials	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO feature can be utilized by remote users to connect to internal resources. Enabled

Example

The following example shows a simple VIA connection profile:

```
(host) [md] (config) #aaa authentication via connection-profile "via"
(host) [md] (VIA Connection Profile "via") #server addr 202.100.10.100 internal-ip
10.11.12.13 desc "VIA Primary" position 0
(host) [md] (VIA Connection Profile "via") #auth-profile "default" position 0
(host) [md] (VIA Connection Profile "via") #tunnel address 10.0.0.0 netmask
255.255.255.0
(host) [md] (VIA Connection Profile "via") #split-tunneling
(host) [md] (VIA Connection Profile "via") #windows-credentials
(host) [md] (VIA Connection Profile "via") #client-netmask 255.0.0.0
(host) [md] (VIA Connection Profile "via") #dns-suffix-list mycorp.com
(host) [md] (VIA Connection Profile "via") #dns-suffix-list example.com
(host) [md] (VIA Connection Profile "via") #support-email via-support@example.com
(host) [md] (VIA Connection Profile "via") #certificate-criteria
certificateIssuer="HPE Root CA"; 2.5.4.10=SmartCard;
emailAddress=support@example.com
```

The following CLI commands configure the **tos-dscp** parameter:

```
(host) [mynode] (config) #aaa authentication via connection-profile <profile-name>
(host) [mynode] (VIA Connection Profile "<profile-name>") #tos-dscp <0-63>
```

The following CLI commands configure IPv6 address of the managed device:

```
(host) [mynode] (config) #aaa authentication via connection-profile test
(host) [mynode] (VIA Connection Profile "test") #server addr 2001:1:2:2020::1
internal-ip 10.11.12.13 desc "VIA Primary" position 0
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The following terminologies are updated: <ul style="list-style-type: none">▪ All instances of <code>blacklist</code> have been replaced with <code>denylist</code>.▪ All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.7.0.0	The <code>addr</code> sub-parameter was modified to include IPv6 address.
ArubaOS 8.4.0.0	The <code>l2-forwarding</code> parameter was added.
ArubaOS 8.3.0.0	The <code>tos-dscp</code> parameter was added.
ArubaOS 8.1.0.0	The <code>certificate-criteria</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication via global-config

```
aaa authentication via global-config
no
ssl-fallback-enable
max-via-vpn-sessions
no max-via-vpn-sessions
```

Description

The global config option allows you to enable SSL fallback mode. If the SSL fallback mode is enabled, the VIA client will use SSL to create a secure connection.

Parameter	Description
no	Disables SSL fallback option.
ssl-fallback-enable	Use this option to enable an SSL fallback connection.
max-via-vpn-sessions	Sets the value of maximum concurrent VIA VPN sessions per user. Range: 1-32. Default: 0
no max-via-vpn-sessions	Resets the value of maximum concurrent VIA VPN sessions per user to 0.

Example

```
(host) [md] (config) #aaa authentication via global-config
(host) [md] (VIA Global Configuration) #max-via-vpn-sessions
<max-via-vpn-sessions> Maximum Concurrent VIA VPN Sessions Per User. Range: 1-32.
Default: 0 (Disabled).
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The max-via-vpn-sessions parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor in the managed device node.

aaa authentication via web-auth

```
aaa authentication via web-auth default
  auth-profile <auth-profile> position <position>
  clone <source>
  no
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (<https://<server-IP-address>/via>) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Parameter	Description
auth-profile <auth-profile>	The name of the VIA authentication profile
position <position>	The position of the profile to specify the order of selection.
clone <source>	Duplicate an existing authentication profile.

Example

```
(host) [md] (config) #aaa authentication via web-auth default
(host) [md] (VIA Web Authentication "default") #auth-profile default position 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication vpn

```
aaa authentication vpn <profile-name>
  cert-cn-lookup
  clone <source>
  default-role <guest>
  export-route
  max-authentication-failures <number>
  no ...
  pan-integration
  radius-accounting
  server-group <group>
  user-idle-timeout
```

Description

This command configures VPN authentication settings.

Parameter	Description
<profile-name>	There are three VPN profiles: default , default-rap or default-cap . This allows users to use different AAA servers for VPN, Remote AP and Campus AP clients. The default and default-rap profiles are configurable. The default-cap profile is not configurable and is predefined with the default settings.
cert-cn-lookup	If you use client certificates for user authentication, enable this option to verify that the CN of the certificate exists in the server. This parameter is enabled by default in the default-cap and default-rap VPN profiles, and disabled by default on all other VPN profiles.
clone <source>	Copies data from another VPN authentication profile. Source is the profile name from which the data is copied.
default-role <role>	Role assigned to the VPN user upon login. This parameter requires PEF for VPN Users license. guest
export-route	Exports a VPN IP address as a route to the external world. enabled
max-authentication-failures <number>	Maximum number of authentication failures before the user is blacklisted/denylister. The supported range is 1-10 failures. A value of 0 disables blacklisting/denylister. This parameter requires the RFProtect license. 0
no	Negates any configured parameter.
pan-integration	Require IP mapping at Palo Alto Networks firewalls. disabled

Parameter	Description
radius-accounting	Configure server group for RADIUS accounting
server-group <group>	Name of the group of servers used to authenticate VPN users. internal
user-idle-timeout	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.

Usage Guidelines

This command configures VPN authentication settings for VPN, Remote AP and Campus AP clients. Use the `vpdn group` command to configure L2TP or IPsec or a PPTP VPN connection.

Example

The following command configures VPN authentication settings for the default-rap profile:

```
(host) ^[md] (config) #aaa authentication vpn default-rap
(host) ^[md] (VPN Authentication Profile "default-rap")default-role guest
(host) ^[md] (VPN Authentication Profile "default-rap")clone default
(host) ^[md] (VPN Authentication Profile "default-rap")max-authentication-failures
0
(host) ^[md] (VPN Authentication Profile "default-rap")server-group vpn-server-
group
```

The following message appears when a user tries to configure the non-configurable default-cap profile:

```
(host) ^[md] (config) #aaa authentication vpn default-cap
Predefined VPN Authentication Profile "default-cap" is not editable
```

The following example describes the steps to use the CLI to configure a VPN for Cisco Smart Card Clients using certificate authentication and IKEv1, where the client is authenticated against user entries added to the internal database:

```
(host) ^[md] (config) #aaa authentication vpn default
server-group internal
(host) ^[md] (config) #no crypto-local isakmp xauth
(host) ^[md] (config) #vpdn group l2tp
enable
client dns 101.1.1.245
(host) ^[md] (config) #ip local pool sc-clients 10.1.1.1 10.1.1.250
(host) ^[md] (config) #crypto-local isakmp server-certificate MyServerCert
(host) ^[md] (config) #crypto-local isakmp ca-certificate TrustedCA
(host) ^[md] (config) #crypto isakmp policy 1
authentication rsa-sig
```

The following command configures client entries in the internal database:

```
(host) [mynode] #local-userdb add username <name> password <password>
```

The following example configures a VPN for XAuth IKEv1 clients in config mode using a username and password:

```
(host) ^[md] (config) #aaa authentication vpn default
server-group internal
crypto-local isakmp xauth
(host) ^[md] (config) #vpdn group l2tp
enable
client dns 101.1.1.245
(host) ^[md] (config) #ip local pool pw-clients 10.1.1.1 10.1.1.250
(host) ^[md] (config) #crypto isakmp key 0987654 address 0.0.0.0 netmask 0.0.0.0
(host) ^[md] (config) #crypto isakmp policy 1
authentication pre-share
```

Enter the following command to configure client entries in the internal database:

```
(host) [mynode] #local-userdb add username <name> password <password>
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters. The default-role parameter requires PEF for VPN Users license.	Config mode on Mobility Conductor.

aaa authentication wired

```
aaa authentication wired
  blacklist-time / denylist-time <timer>
  no ...
  profile <aaa-profile>
```

Description

This command configures authentication for a client device that is directly connected to a port on the managed device. It also references an AAA profile that is configured for MAC or 802.1X authentication. The port on the managed device to which the device is connected must be configured as untrusted.

Parameter	Description
<code>blacklist-time / denylist-time <timer></code>	Sets the time to block the user. Range: 1-65535 seconds. Default: 3600 seconds.
<code>no</code>	Negates any configured parameter.
<code>profile <aaa-profile></code>	Name of the AAA profile that applies to wired authentication. This profile must be configured for a Layer-2 authentication, either 802.1X or MAC.

Example

The following commands configure an AAA profile for 802.1X authentication and a wired profile that references the AAA profile:

```
(host) ^[md] (config) aaa profile sec-wired
dot1x-default-role employee
dot1x-server-group sec-svrs
(host) ^[md] (config) aaa authentication wired
profile sec-wired
```

Related Commands

Command	Description
vlan	Assign an AAA profile to an individual VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	The <code>blacklist-time</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa authentication wispr

```
aaa authentication wispr
  agent string
  clone <source>
  default-role <role>
  logon-wait {cpu-threshold <cpu-threshold>}|{maximum-delay <maximum-delay>}|{minimum-
delay <minimum-delay>}
  no ...
  max-authentication-failures
  server-group <server-group>
  wispr-location-id-ac <wispr-location-id-ac>
  wispr-location-id-cc <wispr-location-id-cc>
  wispr-location-id-isocc <wispr-location-id-isocc>
  wispr-location-id-network <wispr-location-id-network>
  wispr-location-name-location <wispr-location-name-location>
  wispr-location-name-operator-name <wispr-location-name-operator>
```

Description

This command configures WISPr authentication with the WISPr RADIUS server of an ISP.

WISPr authentication allows a smart client to remain authenticated on the network when they roam between WISPs, even if the wireless hotspot uses an ISP for which the client may not have an account.

If you are hotspot operator using WISPr authentication, and a client that has an account with your ISP attempts to access the Internet at your hotspot, then your ISP's WISPr AAA server authenticates that client directly, and allows the client access on the network. If, however, the client only has an account with a partner ISP, then your ISP's WISPr AAA server will forward that client's credentials to the partner ISP's WISPr AAA server for authentication. Once the client has been authenticated on the partner ISP, it will be authenticated on your hotspot's own ISP, as per their service agreements. Once your ISP sends an authentication message to the managed device, the managed device assigns the default WISPr user role to that client.

ArubaOS supports the following smart clients, which enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification redirect, proxy, authentication and logoff messages within HTML messages to the managed device.

- iPass
- Boingo
- Rustive
- eRoam
- T&T

A WISPr authentication profile includes parameters to define RADIUS attributes, the default role for authenticated WISPr users, maximum numbers of authenticated failures and logon wait times. The WISPr-Location-ID sent from the managed device to the WISPr RADIUS server will be the concatenation of the ISO Country Code, E.164 Country Code, E.164 Area Code and SSID or Zone parameters configured in this profile.

The parameters to define WISPr RADIUS attributes are specific to the RADIUS server your ISP uses for WISPr authentication; contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites www.iso.org and www.itu.int.

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, you must also configure the **NAS identifier** parameter in the RADIUS server profile for the WISPr server

Parameter	Description
<code>agent string</code>	User Agent String to be registered for use in WISPR Profile. Max User Agent String len: 32 characters. Max number of User Agent string: 32.
<code>clone <source></code>	Copy data from another WISPr Authentication Profile.
<code>default-role</code>	Default role assigned to users that complete WISPr authentication.
<code>logon-wait</code>	Configure the CPU utilization threshold that will trigger logon wait maximum and minimum times.
<code>CPU-threshold <cpu-threshold></code>	Percentage of CPU utilization at which the maximum and minimum login wait times are enforced. Range: 1-100%. Default: 60%.
<code>max-authentication-failures</code>	Maximum auth failures before user is blacklisted/denylister. Range: 0-10. Default: 0.
<code>maximum-delay <maximum-delay></code>	If the CPU utilization of a managed device has surpassed the CPU-threshold value, the <code>maximum-delay</code> parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
<code>minimum-delay <minimum-delay></code>	If the CPU utilization of a managed device has surpassed the CPU-threshold value, the <code>minimum-delay</code> parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
<code>wispr-location-id-ac <wispr-location-id-ac></code>	The E.164 Area Code in the WISPr Location ID.
<code>wispr-location-id-cc <wispr-location-id-cc></code>	The 1-3 digit E.164 Country Code in the WISPr Location ID.
<code>wispr-location-id-isocc <wispr-location-id-isocc></code>	The ISO Country Code in the WISPr Location ID.
<code>wispr-location-id-network <wispr-location-id-network></code>	The SSID or network name in the WISPr Location ID.
<code>wispr-location-name-location <wispr-location-name-location></code>	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
<code>wispr-location-name-operator-name <wispr-location-name-operator></code>	A name identifying the hotspot operator.

Example

The following commands configure an WISPr authentication profile:

```
(host) ^[md] (config) aaa authentication wispr
default-role authuser
max-authentication-failures 5
server-group wisprl
```

```
wispr-location-id-ac 408
wispr-location-id-cc 1
wispr-location-id-isoccc us
wispr-location-id-network <wispr-location-id-network>
wispr-location-name-location <wispr-location-name-location>
wispr-location-name-operator-name <wispr-location-name-location>
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa bandwidth-contract

```
aaa bandwidth-contract <name> {kbits <kbits>}|{mbits <mbits>}|{percentage <percentage>}
```

Description

This command configures a bandwidth contract. You can apply a configured bandwidth contract to a user role or to a VLAN. When you apply a bandwidth contract to a user role (see [user-role on page 4060](#)), you specify whether the contract applies to upstream traffic (from the client to the managed device) or downstream traffic (from the managed device to the client). You can also specify whether the contract applies to all users in a specified user role or per-user in a user role.

When you apply a bandwidth contract to a VLAN (see [interface vlan on page 776](#)), the contract limits multicast traffic and does not affect other data. This is useful because an AP can only send multicast traffic at the rate of the slowest associated client. Thus excessive multicast traffic will fill the buffers of the AP, causing frame loss and poor voice quality. Generally, every system should have a bandwidth contract of 1 Mbps or even 700 Kbps and it should be applied to all VLANs with which users are associated, especially those VLANs that pass through the upstream router. The exception are VLANs that are used for high speed multicasts, where the SSID is configured without low data rates.

Parameter	Description
<name>	Name that identifies this bandwidth contract.
kbits <kbwm>	Limit the traffic rate for this bandwidth contract to a specified number of Kbps. 256-2000000
mbits <mbwm>	Limit the traffic rate for this bandwidth contract to a specified number of Mbps. 1-2000
percentage <pbwm>	Specify bandwidth as percentage of link capacity. 1-100

Example

The following commands configure a set of bandwidth contracts, then apply those contracts to all upstream and downstream traffic except for the echo, icmp, iperf, icmp6, and synflood applications, and the web, streaming, peer-to-peer, unified-communication, and tunneling application categories.

```
(host) ^[md] (config) #aaa bandwidth-contract up-256k-1 kbits 256
(host) ^[md] (config) #aaa bandwidth-contract up-512k-1 kbits 512
(host) ^[md] (config) #aaa bandwidth-contract up-1m-1 mbits 1
(host) ^[md] (config) #aaa bandwidth-contract up-5m-1 mbits 5
(host) ^[md] (config) #aaa bandwidth-contract up-10m-1 mbits 10
(host) ^[md] (config) #aaa bandwidth-contract up-20m-1 mbits 20
(host) ^[md] (config) #aaa bandwidth-contract up-50m-1 mbits 50
(host) ^[md] (config) #aaa bandwidth-contract up-100m-1 mbits 100
(host) ^[md] (config) #aaa bandwidth-contract up-500m-1 mbits 500
(host) ^[md] (config) #aaa bandwidth-contract up-1000m-1 mbits 1000
```

```
(host) ^[md] (config) #aaa bandwidth-contract dw-256k-1 kbits 256
(host) ^[md] (config) #aaa bandwidth-contract dw-512k-1 kbits 512
(host) ^[md] (config) #aaa bandwidth-contract dw-1m-1 mbits 1
(host) ^[md] (config) #aaa bandwidth-contract dw-5m-1 mbits 5
(host) ^[md] (config) #aaa bandwidth-contract dw-10m-1 mbits 10
(host) ^[md] (config) #aaa bandwidth-contract dw-20m-1 mbits 20
(host) ^[md] (config) #aaa bandwidth-contract dw-50m-1 mbits 50
(host) ^[md] (config) #aaa bandwidth-contract dw-100m-1 mbits 100
(host) ^[md] (config) #aaa bandwidth-contract dw-500m-1 mbits 500
(host) ^[md] (config) #aaa bandwidth-contract dw-1000m-1 mbits 1000
(host) ^[md] (config) #interface gigabitethernet 0/0/1
```

Related Commands

Command	Description
interface gigabitethernet	Use this command to apply a bandwidth contract to downstream or upstream traffic on a specified interface.
show aaa bandwidth-contracts	Use this command to view contracts to limit traffic for a user or VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa dns-query-interval

```
aaa dns-query-interval <minutes>
```

Description

Configure how often the managed device should generate a DNS request to cache the IP address for a RADIUS server identified via its FQDN.

If you define a RADIUS server using the FQDN of the server rather than its IP address, the managed device will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to configure the frequency of these requests.

Parameter	Description
<minutes>	Specify, in minutes, the interval between DNS requests sent from the managed device to the DNS server. 1-1440 minutes 1 minute

Example

This command configures a DNS query interval of 30 minutes.

```
(host) ^[md] (config)# aaa dns-query-interval 30
```

Related Commands

Command	Description
show aaa dns-query-interval	This command is used to view the current DNS query interval.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa derivation-rules

```
aaa derivation-rules user <name>
  no ...
  set {role|vlan} condition <rule-type> <attribute> <value> set-value {<role>|<vlan>}
  [description <rule description>][position <number>]
```

Description

This command configures rules which assigns a AAA profile, user role or VLAN to a client based upon the client's association with an AP.

A user role cannot be assigned by an AAA derivation rule unless the managed device has a PEFNG license.

Parameter	Description
<name>	Name that identifies this set of UDRs.
no	Negates a configured rule.
set {role vlan}	Specify whether the action of the rule is to set the role or the VLAN.
condition	Condition that should be checked to derive role or VLAN.
<rule-type>	For a rule that sets an AAA profile, use the user-vlan rule type. For a role or VLAN UDR, select one of the following rules: <ul style="list-style-type: none">■ ssid: BSSID of access point.■ dhcp-option: Use DHCP signature matching to assign a role or VLAN.■ dhcp-option-77: Enable DHCP packet processing.■ encryption-type: Encryption method used by station.■ ssid: ESSID of access point.■ location: user location (AP name).■ macaddr: MAC address of user. If you use the dhcp-option rule type, best practices are to enable the enforce-dhcp option in the AAA profile referenced by Virtual AP profile of the AP group.
<attribute><value>	Specify one of the following conditions: <ul style="list-style-type: none">■ contains: Check if attribute <i>contains</i> the string in the <value> parameter.■ ends-with: Check if attribute <i>ends with</i> the string in the <value> parameter.■ equals: Check if attribute <i>equals</i> the string in the <value> parameter.■ not-equals: Check if attribute <i>is not equal</i> to the string in the <value> parameter.■ starts-with: Check if attribute <i>starts with</i> the string in the <value> parameter.
set-value <role> <vlan>	Specify the user role or VLAN ID to be assigned to the client if the above condition is met.

Parameter	Description
description	Describes the UDR. This parameter is optional and has a 128 character maximum.
position	Position of this rule relative to other rules that are configured.

The user role can be derived from attributes from the client's association with an AP. UDRs are executed before the client is authenticated.

You configure the user role to be derived by specifying condition rules; when a condition is met, the specified user role is assigned to the client. You can specify more than one condition rule; the order of rules is important as the first matching condition is applied. You can also add a description of the rule.

The table below describes the conditions for which you can specify a user role or VLAN.

Rule Type	Condition	Value
bssid: Assign client to a role or VLAN based upon the BSSID of AP to which client is associating.	One of the following: <ul style="list-style-type: none"> contains ends with equals does not equal starts with 	MAC address (xx:xx:xx:xx:xx:xx)
dhcp-option: Assign client to a role or VLAN based upon the DHCP signature ID.	One of the following: <ul style="list-style-type: none"> equals starts with 	DHCP signature ID. This string is <i>not</i> case sensitive.
dhcp-option-77: Assign client to a role or VLAN based upon the user class identifier returned by DHCP server.	equals	string
encryption-type: Assign client to a role or VLAN based upon the encryption type used by the client.	One of the following: <ul style="list-style-type: none"> equals does not equal 	<ul style="list-style-type: none"> Open (no encryption) WPA or WPA2 AES WPA-TKIP (static or dynamic) Dynamic WEP WPA or WPA2 AES PSK Static WEP xSec
essid: Assign client to a role or VLAN based upon the ESSID to which the client is associated.	One of the following: <ul style="list-style-type: none"> contains ends with equals does not equal starts with value of (does not take <i>string</i>; attribute value is used as role) 	string

Rule Type	Condition	Value
location: Assign client to a role or VLAN based upon the AP name to which the client is associated.	One of the following: <ul style="list-style-type: none"> ■ equals ■ does not equal 	string
macaddr: MAC address of the client.	One of the following: <ul style="list-style-type: none"> ■ contains ■ ends with ■ equals ■ does not equal ■ starts with 	MAC address (xx:xx:xx:xx:xx:xx)

The device identification feature allows you to assign a user role or VLAN to a specific device type by identifying a DHCP option and signature for that device. If you create a user rule with the **DHCP-Option** rule type, the first two characters in the **Value** field must represent the hexadecimal value of the DHCP option that this rule should match, while the rest of the characters in the **Value** field indicate the DHCP signature the rule should match. To create a rule that matches DHCP option 12 (host name), the first two characters of the in the **Value** field must be the hexadecimal value of 12, which is 0C. To create a rule that matches DHCP option 55, the first two characters in the **Value** field must be the hexadecimal value of 55, which is 37.

The following table describes some of the DHCP options that are useful for assigning a user role or VLAN.

DHCP Option	Description	Hexadecimal Equivalent
12	Host name	0C
55	Parameter Request List	37
60	Vendor Class Identifier	3C
81	Client FQDN	51

To identify DHCP strings used by an individual device, access the CLI in config mode and issue the following command to include DHCP option values for DHCP-DISCOVER and DHCP-REQUEST frames in the log file of the managed device:

```
logging level debugging network process dhcpd
```

Now, connect the device you want to identify to the network, and issue the CLI command `show log network`. The sample below is an example of the output that may be generated by this command.

Be aware that each device type may not have a unique DHCP fingerprint signature. For example, devices from different manufacturers may use vendor class identifiers that begin with similar strings. If you create a DHCP-Option rule that uses the starts-with condition instead of the equals condition, the rule may assign a role or VLAN to more than one device type.

```
(host) ^[md] (config) #show log network all | include DISCOVER
Feb 26 02:50:34 :202534: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER
00:19:d2:01:0b:84 Options 74:01 3d:010019d2010b84
0c:736861626172657368612d39393730 3c:4d53465420352e30 37:010f03062c2e2f1f21f92b
Feb 26 02:50:42 :202534: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER
00:19:d2:01:0b:84 Options 74:01 3d:010019d2010b84
0c:736861626172657368612d39393730 3c:4d53465420352e30 37:010f03062c2e2f1f21f92b
Feb 26 02:50:42 :202534: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER
00:19:d2:01:0b:84 Options 74:01 3d:010019d2010b84
0c:736861626172657368612d39393730 3c:4d53465420352e30 37:010f03062c2e2f1f21f92b
Feb 26 02:53:03 :202534: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan10: DISCOVER
00:26:c6:52:6b:7c Options 74:01 3d:010026c6526b7c 0c:41525542412d46416c73653232
3c:4d53465420352e30 37:010f03062c2e2f1f21f92b 2b:dc00
...

(host) ^[md] (config) #show log network all| include REQUEST
Feb 26 02:53:04 :202536: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST
00:26:c6:52:6b:7c reqIP=10.10.10.254 Options 3d:010026c6526b7c 36:0a0a0a02
0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
Feb 26 02:53:04 :202536: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST
00:26:c6:52:6b:7c reqIP=10.10.10.254 Options 3d:010026c6526b7c 36:0a0a0a02
0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
Feb 26 02:56:02 :202536: <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST
00:26:c6:52:6b:7c reqIP=10.10.10.254 Options 3d:010026c6526b7c
0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
```

Examples

The following command sets the client's user role to "guest" if the client associates to the "Guest" ESSID. The rule description indicates that it was created for special customers.

```
(host) ^[md] (config) aaa derivation-rules user derive1
set role condition essid equals Guest set-value guest description
createdforspecialcustomers
```

The example rule shown below sets a user role for clients whose host name (DHCP option 12) has a value of 6C6170746F70, which is the hexadecimal equivalent of the ASCII string "laptop". The first two digits in the Value field are the hexadecimal value of 12 (which is 0C), followed by the specific signature to be matched.

```
(host) ^[md] (config) aaa derivation-rules user device-role
set role condition dhcp-option equals 0C6C6170746F70 set-value laptop_role
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system. The PEFNG license must be installed for a user role to be assigned.	Config mode on Mobility Conductor.

aaa inservice

```
aaa inservice <server-group> <server>
```

Description

This command designates an out of service authentication server to be in service.

By default, Mobility Conductor marks an unresponsive authentication server as “out of service” for a period of 10 minutes (you can set a different time limit with the `aaa timers dead-time` command). The `aaa inservice` command is useful when you become aware that an “out of service” authentication server is again available before the dead-time period has elapsed. You can use the `aaa test-server` command to test the availability and response of a configured authentication server.

Parameter	Description
<server-group>	Server group to which this server is assigned.
<server>	Name of the configured authentication server.

Example

The following command sets an authentication server to be in service:

```
aaa inservice corp-rad rad1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.Mobility Conductor

aaa ipv6 user add

```
aaa ipv6 user add <ipv6addr>
  authentication-method {dot1x|stateful-dot1x}
  mac <macaddr>
  name <username>
  profile <aaa-profile>
  role <role>
```

Description

This command should only be used for troubleshooting issues with a specific IPv6 client. This command manually assigns a user role or other values to a specified IPv6 client. For example, you can create a role debugging that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the debugging role to a specific client. Use the `aaa ipv6 user delete` command to remove the client or device from the role.

Issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the `aaa ipv6 user clear-sessions` command to clear ongoing sessions.

Parameter	Description
<ipv6addr>	IPv6 address of the user to be added.
authentication-method	Authentication method for the client.
dot1x	802.1X authentication.
stateful-dot1x	Stateful 802.1X authentication.
mac <macaddr>	MAC address of the client.
name <username>	Name of the client.
profile <aaa-profile>	AAA profile for the client.
role <role>	User role for the client.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific IPv6 client:

```
(host) [\md] (config) #ip access-list session ipv6-log-https
(host) [\md] (config-submode) #any any svc-https permit log
(host) [\md] (config) #user-role ipv6-web-debug
(host) [\md] (config-submode) #session-acl ipv6-log-https
(host) [\md] (config) #aaa ipv6 user add 2002:d81f:f9f0:1000:e409:9331:1d27:ef44 role
ipv6-web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa ipv6 user clear-sessions

```
aaa ipv6 user clear-sessions <ipaddr>
```

Description

This command clears any ongoing sessions that the client already had before being assigned a role with the `aaa ipv6 user add` command.

Parameter	Description
<ipv6addr>	IPv6 address of the client.

Example

The following command clears ongoing sessions for an IPv6 client:

```
(host) [/md] (config) #aaa user clear-sessions  
2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa ipv6 user delete

```
aaa ipv6 user delete {<ipv6addr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command allows you to manually delete clients, users, or roles. For example, if you used the `aaa ipv6 user add` command to assign a user role to an IPv6 client, you can use this command to remove the role assignment.

Parameter	Description
<ipv6addr>	IPv6 address of the client to be deleted.
all	Deletes all connected IPv6 clients.
mac <macaddr>	MAC address of the IPv6 client to be deleted.
name <username>	Name of the IPv6 client to be deleted.
role <role>	Role of the IPv6 client to be deleted.

Example

The following command a role:

```
(host) [/md] (config) #aaa ipv6 user delete role web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa ipv6 user logout

```
aaa ipv6 user logout <ipv6addr>
```

Description

This command logs out an authenticated IPv6 client. The client must reauthenticate.

Parameter	Description
<ipv6addr>	IPv6 address of the client to be logged out.

Example

The following command logs out an IPv6 client:

```
(host) [/md] (config) #aaa user logout 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa log

[no] aaa log

Description

Enable per-user log files for AAA events.

By default, logging is always enabled. Issue the `no aaa log` command to disable per-user logging and re-enable it again using the command `aaa log`.

Example

The example below enables per-user AAA log files.

```
(host) ^[md] (config) #aaa log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa profile

```
aaa profile <profile>
  ageout-bridge-user
  authentication-dot1x <dot1x-profile>
  authentication-mac <mac-profile>
  clone <profile>
  devtype-classification
  dh-groups
  dot1x-default-role <role>
  dot1x-server-group <group>
  download-role
  enforce-dhcp
  initial-role <role>
  l2-auth-fail-through
  mac-default-role <role>
  mac-server-group <group>
  max-ip ipv4 wireless <max_ipv4_users>
  multiple-server-accounting
  no ...
  open ssid radius accounting
  pan-integration
  radius-accounting <group>
  radius-acct-session-id-in-access
  radius-interim-accounting
  radius-roam-accounting
  reauth-wired-user-vlan-change
  rfc-3576-server <ipaddr>
  user-derivation-rules <profile>
  user-idle-timeout
  username-from-dhcp-opt12
  wired-to-wireless-roam
  xml-api-server <ipaddr>
```

Description

This command configures the authentication for a WLAN.

Parameter	Description
<profile>	Name that identifies this instance of the profile. The name must be 1-63 characters. default
ageout-bridge-user	Enables ageout mechanism for wireless clients in bridge mode.
authentication-dot1x <dot1x-profile>	Name of the 802.1X authentication profile associated with the WLAN.
authentication-mac <mac-profile>	Name of the MAC authentication profile associated with the WLAN.
clone <profile>	Name of an existing AAA profile configuration from which parameter values are copied.

Parameter	Description
<code>devtype-classification</code>	The device identification feature can automatically identify different client device types and operating systems by parsing the User-Agent strings in a client's HTTP packets. When the <code>devtype-classification</code> parameter is enabled, the output of the <code>show user</code> and <code>show user-table</code> commands shows each client's device type, if that client device can be identified. enabled
<code>dh-groups</code>	Set supported D-H groups for EnhancedOpen
<code>dot1x-default-role <role></code>	Configured role assigned to the client after 802.1X authentication. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. This parameter requires the PEFNG license. guest
<code>dot1x-server-group <group></code>	Name of the server group used for 802.1X authentication.
<code>download-role</code>	Enables role download from ClearPass Policy Manager if not defined. 2
<code>enforce-dhcp</code>	When you enable this option, clients must complete a DHCP exchange to obtain an IP address. disabled
<code>initial-role <role></code>	Role for unauthenticated users. logon
<code>l2-auth-fail-through</code>	To select different authentication method if one fails. disabled
<code>mac-default-role <role></code>	Configured role assigned to the user when the device is MAC authenticated. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. This parameter requires the PEFNG license. guest
<code>mac-server-group group</code>	Name of the server group used for MAC authentication.
<code>max-ip ipv4 wireless <max_ipv4_users></code>	Control the number of IPv4 addresses that can be associated to single wireless user. Increasing the max-ip limit may prevent the system from scaling to maximum users on all Mobility Conductor or managed devices. Range: 1-32 2
<code>multiple-server-accounting</code>	If enabled, the Mobility Conductor sends RADIUS accounting to all servers in RADIUS accounting server group. disabled

Parameter	Description
no	Negates any configured parameter.
open ssid radius accounting	Initiates RADIUS accounting as soon as the user associates to an Open SSID without any authentication. Do not enable this parameter for wired users. If enabled, the Mobility Conductor sends RADIUS accounting packets for unauthenticated wired users. disabled
pan-integration	The profile requires mapping at a Palo Alto Networks (PAN) firewall. disabled
radius-accounting <group>	Name of the server group used for RADIUS accounting.
radius-acct-session-id-in-access	Use this to include Acct-Session-Id in RADIUS Access-Request.
radius-interim-accounting	By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. Issue the interim-radius-accounting command to allow the managed device to send Interim-Update messages with current user statistics to the server at regular intervals. disabled
rfc-3576-server <ip-addr>	IPv4 or IPv6 address of a RADIUS server that can send user disconnect, session timeout and CoA messages, as described in RFC 3576, Dynamic Authorization Extensions to RADIUS. This parameter requires the PEFNG license.
radius-roam-accounting	Enable the managed device to send Interim-Update messages (without user statistics) to the server, when a client roams to a different AP.
reauth-wired-user-vlan-change	When a wired user moves across VLANs, a trigger is created to reauthenticate this user. Enabled
user-derivation-rules <profile>	User attribute profile from which the user role or VLAN is derived.
user-idle-timeout	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used. disabled
username-from-dhcp-opt12	Enter a username from dhcp option 12 for non-802.1X users.
wired-to-wireless-roam	Keeps user authenticated when roaming from the wired side of the network. enabled

Parameter	Description
<code>xml-api-server <ip-addr></code>	IP address of a configured XML API server. This parameter requires the PEFNG license.

The AAA profile defines the user role for unauthenticated users, the default user role for MAC or 802.1X authentication, and UDRs. The AAA profile contains the authentication profile and authentication server group.

There are predefined AAA profiles available, `default-dot1x`, `default-mac-auth`, and `default-open`. These profiles have the parameter values shown in the following table.

Parameter	<code>default-dot1x</code>	<code>default-mac-auth</code>	<code>default-open</code>
<code>authentication-dot1x</code>	default	N/A	N/A
<code>authentication-mac</code>	N/A	default	N/A
<code>dot1x-default-role</code>	authenticated	guest	guest
<code>dot1x-server-group</code>	N/A	N/A	N/A
<code>initial-role</code>	logon	logon	logon
<code>mac-default-role</code>	guest	authenticated	guest
<code>mac-server-group</code>	default	default	default
<code>radius-accounting</code>	N/A	N/A	N/A
<code>rfc-3576-server</code>	N/A	N/A	N/A
<code>user-derivation-rules</code>	N/A	N/A	N/A
<code>wired-to-wireless roam</code>	enabled	enabled	enabled

Changing the `max-ip ipv4 wireless` parameter from the default value is recommended for special deployments. If your WLAN has multiple device IP associated to single MAC address, you can increase the this value from the default value of 2.

The default value is 2 IPv4 users per wireless user. Total number of IPv4 users created can be a maximum of two times the license. If you configure 32 `max-ip IPv4 users` , total number of IPv4 users is 32 times the license. This can prevent the managed device from scaling to the maximum limit of IP users. Total number of IPv4 users should be scaled down to offset this issue.

Increasing the value of the `max-ip ipv4 wireless` parameter may increase the look-up time due to an increase in the creation and deletion of IPv4 users on the managed device. In a deployment where there is Captive Portal and 802.1X authentication implemented, increasing the number of IPv4 users can further deplete performance.

Example

The following command configures an AAA profile that assigns the employee role to clients after they are authenticated using the 802.1X server group `radiusnet`.

```
(host) ^[md] (config) #aaa profile corpnet
(host) ^[md] (AAA Profile "corpnet")dot1x-default-role employee
(host) ^[md] (AAA Profile "corpnet")dot1x-server-group radiusnet
```

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>ageout-bridge-user</code> parameter was introduced.
ArubaOS 8.5.0.0	The <code>rfc-3576-server <ipaddr></code> parameter was updated to also support IPv6 address of the server.
ArubaOS 8.3.0.0	The <code>reauth-wired-user-vlan-change</code> parameter was added.
ArubaOS 8.1.0.0	The <code>radius-roam-accounting</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

aaa password-policy mgmt

```
aaa password-policy mgmt
  certificate-lock-out
  certificate-lock-out-time
  enable
  min-char-difference
  no
  password-lock-out
  password-lock-out-time
  password-max-character-repeat.
  password-min-digit
  password-min-length
  password-min-lowercase-characters
  password-min-special-character
  password-min-uppercase-characters
  password-not-username
```

Description

Defines a policy for creating management user passwords. By default, the password for a management user has no requirements other than a minimum length of 6 alphanumeric or special characters. You do not need to configure a different management user password policy unless your company enforces a best practices password policy for management users with root access to network equipment.

Parameter	Description
certificate-lock-out	Configure the number of failed attempts within 3 minute window to lockout the user. Provides ability to reduce the number of login attempts that can be made in a short time. Automatically clears the lockout at the end of configured lock-out period. Range: 0-10 attempts. Default: 0 (By default, the user lockout feature is disabled)
certificate-lock-out-time	Configure the number of minutes for which the user is locked out. The lockout is cleared without administrator intervention. Range: 1 min to 1440 min (24 hrs). Default: 3 min.
enable	Enable the password management policy.
password-lock-out	The number of failed attempts within a 3 minute window that causes the user to be locked out for the period of time specified by the password-lock-out-time parameter. Range: 0-10 attempts. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
password-lock-out-time	The number of minutes a user who has exceeded the maximum number of failed password attempts is locked out of the network. After this period has passed, the lockout is cleared without administrator intervention.

Parameter	Description
	<p>When a management user gets locked out, that event is logged in the managed device log file. The management user lockout warning message can have any one of the following warning IDs.</p> <ul style="list-style-type: none"> ■ 125060 = Password policy locked out a management user created via the <code>mgmt-user</code> command in the serial console CLI. ■ 125061 = Password policy locked out a management user created via the WebUI or the <code>mgmt-user</code> command in the Telnet or SSH CLI. ■ 133109 = Password policy locked out a management user created via the <code>local-userdb</code> command in the CLI. <p>Range: 1-1440 3</p>
<code>password-max-character-repeat</code>	<p>The maximum number of consecutive repeating characters allowed in a management user password.</p> <p>Range: 0-10 characters. By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.</p>
<code>password-min-digit</code>	<p>The minimum number of numeric digits required in a management user password.</p> <p>Range: 0-10 digits. By default, there is no requirement for numerical digits in a password, and the parameter has a default value of 0.</p>
<code>password-min-length</code>	<p>The minimum number of characters required for a management user password</p> <p>Range: 6-64 characters. Default: 6.</p> <p>Starting from ArubaOS 8.10.0.0, the range of characters in the management user password is increased from 6-64 to 6-128.</p>
<code>password-min-lowercase-characters</code>	<p>The minimum number of lowercase characters required in a management user password.</p> <p>Range: 0-10 characters. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.</p>
<code>password-min-special-characters</code>	<p>The minimum number of special characters (!, @, #, \$, %, ^, &, *, <, >, {, }, [,], :, ., comma, , +, ~, `) in password. Range: 0-10 special characters.</p> <p>Default: 0 (minimum number of special character required is disabled by default, The following ('), ' (; , - , space, =, /, ?) are dis-allowed).</p>
<code>password-min-special-character</code>	<p>The minimum number of special characters required in a management user password.</p> <p>Range: 0-10 characters. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0. See Usage Guidelines below for a list of allowed and disallowed special characters</p>
<code>password-min-uppercase-characters</code>	<p>The minimum number of uppercase characters required in a management user password.</p>

Parameter	Description
	Range: 0-10 characters. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.
password-not-username	Password cannot be the current username or the username spelled backwards of the management user.

Example

The following command sets a management password policy that requires the password to have a minimum of nine characters, including one numerical digit and one special character:

```
(host) ^[md] (config) aaa password-policy mgmt
enable
password-min-digit 1
password-min-length 9
password-min-special-characters 1
```

Related Commands

Command	Description
show aaa password-policy mgmt	This command displays the current management password policy.

Command History

Release	Modification
ArubaOS 8.10.0.0	The range of characters in the management user password is increased from 6-64 to 6-128.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa query-user

```
aaa query-user <auth-server> <user-name> <mac-address>
```

Description

Troubleshoot an authentication failure by verifying that the user exists in the authentication server database. If the Admin-DN binds successfully but the wireless user fails to authenticate, issue this command to troubleshoot whether the problem is with the wireless network, the managed device, or the authentication server. The `aaa query-user <auth_server> <username> <mac-address>` command to make the managed device sends a search query to find the user. If that search fails in spite of the user being in the server database, it is most probable that the base DN where the search was started was not correct. In such case, it is advisable to make the base DN at the root of the authentication server tree.

Parameter	Description
<auth-server>	Name of a configured authentication server.
<user-name>	Name of a user whose authentication record you want to view.
<mac-address>	MAC address of the client.

Example

The example below shows part of the output for an LDAP record for the username JDOE.

```
(host) [mynode] #aaa query-user eng JDOE
(host) [mynode] #objectClass: top
(host) [mynode] #objectClass: person
(host) [mynode] #objectClass: organizationalPerson
(host) [mynode] #objectClass: user
(host) [mynode] #cn: John Doe
(host) [mynode] #sn: Doe
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012H\011\333K
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012J\350\346F
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\023\001\017\240
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\031\224\030
(host) [mynode] #userCertificate:
0\202\005~0\202\004f\240\003\002\001\002\002\012\031\223\246\022
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\037\177\374\305
(host) [mynode] #givenName: JDE
(host) [mynode] #distinguishedName: CN=John Doe,CN=Users,DC=eng,DC=net
(host) [mynode] #instanceType: 4
(host) [mynode] #whenCreated: 20060516232817.0Z
(host) [mynode] #whenChanged: 20081216223053.0Z
(host) [mynode] #displayName: John Doe
(host) [mynode] #uSNCreated: 24599
(host) [mynode] #memberOf: CN=Cert_Admns,CN=Users,DC=eng,DC=net
```

```
(host) [mynode] #memberOf: CN=ATAC,CN=Users,DC=eng,DC=net
(host) [mynode] #uSNchanged: 377560
(host) [mynode] #department: eng
(host) [mynode] #name: John Doe
...
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa radius-attributes

```
aaa radius-attributes add <attribute> <attribute-id> {date|integer|ipaddr|string} [vendor <name> <vendor-id>]
```

Description

This command configures RADIUS attributes to statically configure values to be included in RADIUS Access-Requests and Accounting-Requests. Add RADIUS attributes for use in SDRs. Use the `show aaa radius-attributes` command to display a list of the current RADIUS attributes recognized by the Mobility Conductor. To add a RADIUS attribute to the list, use the `aaa radius-attributes` command.

Parameter	Description
<code>add <attribute> <attribute-id></code>	Adds the specified attribute name (alphanumeric string), associated attribute ID (integer), and type (date, integer, IP address, or string).
<code>date</code>	Adds a date attribute.
<code>integer</code>	Adds an <code>integer</code> attribute.
<code>ipaddr</code>	Adds an IP address attribute.
<code>string</code>	Adds a string attribute.
<code>vendor</code>	(Optional) Display attributes for a specific vendor name and vendor ID.

Example

The following command adds the VSA Aruba-User-Role:

```
(host) ^[md] (config) aaa radius-attributes add Aruba-User-Role 1 string vendor Arubas 14823
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa radius modifier

```
aaa radius modifier <rad_modifier_name>
  clone <source>
  exclude <name>
  include <name> {[static <static_val>]}[dynamic <ap-group1>|<ap-macaddr1>|<ap-
name1>|<ssid1>|<user-vlan1>|<with>|<ap-group2>|<ap-macaddr2>|<ap-
name2>|<ssid2>|<user-vlan2>]<delimiter>}
no..
```

Description

This command configures the RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server.

Use the `show aaa radius modifier` command to display a list of RADIUS modifier profiles. To create a RADIUS modifier profile with customized attributes, use the `aaa radius-attributes` command.

Parameter	Description
<rad_modifier_name>	The specified RADIUS modifier profile name
clone <source>	Copy data from another Radius Modifier Profile
exclude <name>	Attribute to be excluded in RADIUS request
include <name>	Attribute/Value to be included in RADIUS request
static <static_val>	Static data. (1-128 bytes string in length)
dynamic	First dynamic field. Use the following parameters: <ul style="list-style-type: none">▪ ap-group1: Use AP group as the first dynamic field.▪ ap-macaddr1: Use AP mac address as the first dynamic field.▪ ap-name1: Use AP name as the first dynamic field.▪ ssid1: Use ssid as the first dynamic field.▪ user-vlan1: Use the current VLAN-ID of user as the first dynamic field.
with	(Optional) Connect to the second dynamic field. Use the following parameters: <ul style="list-style-type: none">▪ ap-group2: Use AP group as the second dynamic field.▪ ap-macaddr2: Use AP mac address as the second dynamic field.▪ ap-name2: Use AP name as the second dynamic field.▪ ssid2: Use ssid as the second dynamic field.▪ user-vlan2: Use the current VLAN-ID of user as the second dynamic field.
delimiter	Delimiter (at, colon, dash, dollar, hash, none, percent, semicolon, slash, space) used in the string.
no	Delete Command.

Example

Example for Included attribute

```
(host) [md](config) #aaa radius-attributes add BW-Area-Code 18 integer vendor
Boingo 22472
(host) [md](Radius Modifier Profile "radmodifier1") # include BW-Area-Code static
"212"
(host) [md](Radius Modifier Profile "radmodifier1") # no include BW-Area-Code
```

Example for excluded attribute

```
(host) [md](config) #aaa radius-attributes add BW-Area-Code 18 integer vendor
Boingo 22472
(host) [md](Radius Modifier Profile "radmodifier1") # exclude BW-Area-Code
(host) [md](Radius Modifier Profile "radmodifier1") # no exclude BW-Area-Code
```

Example for modified attribute

Default attributes to carry to radius server can be modified with include option.

```
(host) [md](Radius Modifier Profile "radmodifier1") # include "Aruba-location-id"
static "Shim-office"
```

Command History

Version	Modification
ArubaOS 8.2.0.0	The exclude and include parameters were added.
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa rfc-3576-server

```
aaa rfc-3576-server <ipaddr>
  clone <source>
  enable-radsec
  event-timestamp-requi..
  key <psk>
  no ...
  replay-protection
  window-duration
```

Description

This command configures a RADIUS server that can send user disconnect, session timeout, and CoA messages, as described in RFC 3576, Dynamic Authorization Extensions to RADIUS.

The disconnect, session timeout and change-of-authorization messages sent from the server to managed device contains information to identify the user for which the message is sent. Starting from ArubaOS 8.5.0.0, the managed device also accepts disconnect, session timeout, and CoA message requests from IPv6 address based DAC, and identifies user sessions based on the user's IPv6 address. Managed Device supports the following attributes for identifying the users who authenticate with an RFC 3576 server:

- **user-name:** name of the user to be authenticated
- **framed-ip-address:** user IPv4 address
- **framed-ipv6-address:** user IPv6 address
- **calling-station-id:** phone number of a station that originated a call
- **accounting-session-id:** unique accounting ID for the user session.

If the authentication server sends both supported and unsupported attributes to managed device, the unknown or unsupported attributes will be ignored. If no matching user is found managed device will send a 503: Session Not Found error message back to the RFC 3576 server.

Parameter	Description
<ipaddr>	IPv4 or IPv6 address of the server.
clone <source>	Name of an existing RFC 3576 server configuration from which parameter values are copied.
enable-radsec	Enable RADSEC for the server.
event-timestamp-required	To enable discard of DAC request, if Event-Timestamp is not present in DAC request. This option will only come into the effect, if replay-protection is enabled.
key <psk>	Shared secret to authenticate communication between the RADIUS client and server.
no	Negates any configured parameter.
replay-protection	Enable replay protection for DAC requests.
window-duration	Number in seconds. Default value is 300. This parameter is used:

Parameter	Description
	<ul style="list-style-type: none"> - To check stale DAC requests. - To specify the minimum time-span in seconds between two valid requests with same identifiers, to check replay protection and identify duplicates.

Example

The following command configures an RFC 3576 server:

```
(host) ^[md] (config) aaa rfc-3576-server 10.1.1.245
clone default
key P@$$w0rD;
```

Related Commands

Command	Description
show aaa state user	View information for a user whose session timeout is altered by a RFC 3576 server.

Command History

Release	Modification
ArubaOS 8.5.0.0	The <ipaddr> sub-parameter was updated to also support IPv6 address of the server.
ArubaOS 8.2.0.0	Event-timestamp-required, replay-protection, and window-duration parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa server-group

```
aaa server-group <group>
  allow-fail-through
  auth-server <name> [match-authstring contains|equals|starts-with <string>] [match-fqdn
<string>] [position <number>] [trim-fqdn]
  clone <source>
  load-balance
  no ...
  set role|vlan condition <attribute> contains|ends-with|equals|not-equals|starts-with
<string> set-value <set-value-str> [position <number>]
```

Description

This command allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.

You create a server group for a specific type of authentication or for accounting. The list of servers in a server group is an ordered list, which means that the first server in the group is always used unless it is unavailable (in which case, the next server in the list is used). You can configure servers of different types in a server group, for example, you can include the internal database as a backup to a RADIUS server. You can add the same server to multiple server groups. There is a predefined server group internal that contains the internal database.

Parameter	Description
<group>	Name that identifies the server group. The name must be 32 characters or less.
allow-fail-through	When this option is configured, an authentication failure with the first server in the group causes the Mobility Conductor to attempt authentication with the next server in the list. The Mobility Conductor attempts authentication with each server in the ordered list until either there is a successful authentication or the list of servers in the group is exhausted.
auth-server <name>	Name of a configured authentication server.
match-authstring	This option associates the authentication server with a match rule that the Mobility Conductor can compare with the user or client information in the authentication request. With this option, the user or client information in the authentication request can be in any of the following formats: <domain>\<user> <user>@<domain> host/<pc-name>.<domain> An authentication request is sent to the server only if there is a match between the specified match rule and the user or client information. You can configure multiple match rules for an authentication server.
contains	The rule matches if the user or client information contains the specified string.

Parameter	Description
<code>equals</code>	The rule matches if the user or client information exactly matches the specified string.
<code>starts-with</code>	The rule matches if the user or client information starts with the specified string.
<code>match-fqdn <string></code>	This option associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request. With this option, the user information must be in one of the following formats: <domain>\<user> <user>@<domain>
<code>position <number></code>	Position of the server in the server list. 1 is the top.
<code>trim-fqdn</code>	This option causes the user information in an authentication request to be edited before the request is sent to the server. Specifically, this option: removes the <domain>\ portion for user information in the <domain>\<user> format removes the @<domain> portion for user information in the <user>@<domain> format.
<code>clone <source></code>	Name of an existing server group from which parameter values are copied.
<code>load-balance</code>	Enables load-balancing of authentication requests among different servers in a server group.
<code>no</code>	Negates any configured parameter.
<code>set role vlan</code>	Assigns the client a user role, VLAN ID or VLAN name based on attributes returned for the client by the authentication server. Rules are ordered: the first rule that matches the configured condition is applied. VLAN IDs and VLAN names cannot be listed together.
<code>condition</code>	Attribute returned by the authentication server.
<code>contains</code>	The rule is applied if and only if the attribute value contains the specified string.
<code>ends-with</code>	The rule is applied if and only if the attribute value ends with the specified string.
<code>equals</code>	The rule is applied if and only if the attribute value equals the specified string.
<code>not-equals</code>	The rule is applied if and only if the attribute value is not equal to the specified string.
<code>starts-with</code>	The rule is applied if and only if the attribute value begins with the specified string.
<code>set-value</code>	User role or VLAN applied to the client when the rule is matched.

Parameter	Description
value-of	Sets the user role or VLAN to the value of the attribute returned. The user role or VLAN ID returned as the value of the attribute must already be configured on the Mobility Conductor when the rule is applied.

Example

The following command configures a server group corp-servers with a RADIUS server as the main authentication server and the internal database as the backup. The command also sets the client's user role to the value of the returned Class attribute.

```
(host) ^[md] (config) aaa server-group corp-servers
auth-server radius1 position 1
auth-server internal position 2
set role condition Class value-of
load-balance
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa tacacs-accounting

```
aaa tacacs-accounting
  command {action|all|configuration|show}
  no
  server-group <sg>
```

Description

This command configures reporting of commands issued from a managed device to a TACACS+ server group.

Parameter	Description
command	The types of commands that are reported to the TACACS server group.
action	Reports action commands only.
all	Reports all commands.
configuration	Reports configuration commands only.
show	Reports show commands only.
no	Delete command.
server-group <sg>	The TACACS server group to which the reporting is sent.

Example

The following command enables accounting and reporting of configuration commands to the server-group "tacacs1":

```
(host) [mm] (config) #aaa tacacs-accounting
(host) ^[mm] (config-submode) #server-group tacacs1
(host) ^[mm] (config-submode) #command configuration
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa test-server

```
aaa test-server {mschapv2|pap} <server-name> <username> <passwd> {<STRING>} {<verbose>}
```

Description

This command allows you to check a configured RADIUS authentication server or the internal database. You can use this command to check for an out of service RADIUS server.

Parameter	Description
mschapv2	Use MSCHAPv2 authentication protocol.
pap	Use PAP authentication protocol.
<server-name>	Name of the configured authentication server.
<username>	Username to use to test the authentication server.
<passwd>	Password to use to test the authentication server.
<STRING>	MAC address of the user.
<verbose>	RADIUS server response for a successful or failed authentication.

Example

The following commands add a user in the internal database and verify the configuration:

```
(host) [mynode] #local-userdb add username raduser1 password raduser  
(host) [mynode] #aaa test-server mschapv2 internal raduser1 raduser verbose
```

Starting from ArubaOS 8.1.0, the `aaa test-server` command has a new `verbose` option that displays the RADIUS server's response on a successful or failed authentication.

The following command displays the RADIUS server attributes as returned by the server.

```
(host) [mynode] #aaa test-server mschapv2 internal raduser1 raduser verbose  
Authentication Successful  
Processing time (ms) : 1.397  
Attribute value pairs in response  
-----  
Vendor  Attribute  Value  
-----  -  
MS-CHAPv2  
Role      guest
```

Command History

Release	Modification
ArubaOS 8.1.0.0	The verbose parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa timers

```
aaa timers
  dead-time <minutes>
  idle-timeout <time> [seconds]
  logon-lifetime <0-255>
  stats-timeout <time> [seconds]
```

Description

This command configures the timers that you can apply to clients and servers.

Parameter	Description
dead-time <minutes>	<p>Maximum period, in minutes, that the Mobility Conductor considers an unresponsive authentication server to be out of service.</p> <p>This timer is only applicable if there are two or more authentication servers configured on the Mobility Conductor. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server.</p> <p>If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.</p> <p>0-60 10</p>
idle-timeout <1-15300>	<p>Maximum number of minutes after which a client is considered idle if there is no user traffic from the client.</p> <p>The timeout period is reset if there is a user traffic. If there is no IP traffic in the timeout period or there is no 802.11 traffic as indicated in the station ageout time that is set in the wlan ssid profile, the client is aged out. Once the timeout period has expired, the user is removed immediately and no ping request is sent. If the seconds parameter is not specified, the value defaults to minutes.</p> <p>1-255 5</p>
logon-lifetime	<p>Maximum time, in minutes, that unauthenticated clients are allowed to remain logged on.</p> <p>0-255 5</p>
stats-timeout	<p>User Interim stats timeout value. If the seconds parameter is not specified, the value defaults to minutes. Starting from ArubaOS 8.7.1.3, the range of this parameter has been modified to 1-60.</p> <p>5-60 10</p>

Example

The following command changes the idle time to 10 minutes:

```
(host) ^[md] (config) aaa timers idle-timeout 10
```

Related Commands

Command	Description
show aaa timers	Displays AAA timer values.
show datapath	Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.

Command History

Release	Modification
ArubaOS 8.2.0.0	The range of stats-timeout parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa trusted-ap

aaa trusted-ap <macaddr>

Description

This command configures a trusted non-Aruba AP.

Parameter	Description
<macaddr>	MAC address of the AP.

Example

The following command configures a trusted non-Aruba AP:

```
aaa trusted-ap 00:40:96:4d:07:6e
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa user add

```
aaa user add <ipaddr> [<nusers>] [authentication-method {dot1x|mac|stateful-dot1x|vpn|web}] [mac-addr <macaddr>] [name <username>] [profile <aaa_profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified client or device.

This command should only be used for troubleshooting issues with a specific client or device. This command allows you to manually assign a client or device to a role. For example, you can create a role debugging that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the debugging role to a specific client. Use the `aaa user delete` command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the employee role when you assign them to the debugging role, the client continues any sessions allowed with the employee role. Use the `aaa user clear-sessions` command to clear ongoing sessions.

Parameter	Description
<ipaddr>	IP address of the user to be added.
<nusers>	Number of users to create starting with <ipaddr>.
authentication-method	Authentication method for the user.
dot1x	802.1X authentication.
mac-addr	MAC authentication.
stateful-dot1x	Stateful 802.1X authentication.
vpn	VPN authentication.
web	Captive portal authentication.
mac <macaddr>	MAC address of the user.
name <username>	Name for the user.
profile <aaa_profile>	AAA profile for the user.
role <role>	Role for the user.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific client:

```
(host) [mynode] (config) #ip access-list session log-https
(host) [mynode] (config-submode) #any any svc-https permit log
(host) [mynode] (config-submode) #user-role web-debug
```

```
(host) [mynode] (config-submode) #session-acl log-https
```

In enable mode:

```
(host) [mynode] (config) #aaa user add 10.1.1.236 role web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa user clear-sessions

```
aaa user clear-sessions <ipaddr>
```

Description

This command clears any ongoing sessions that the client already had before being assigned a role with the `aaa user add` command.

Parameter	Description
<ip-addr>	IP address of the user.

Example

The following command clears ongoing sessions for a client:

```
(host) [mynode] (config) #aaa user clear-sessions 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa user delete

```
aaa user delete { |all|<ip-addr>|<ap-ip-addr>|ap-name|mac <macaddr>|name <username>|role <role>}
```

Description

This command allows you to manually delete clients, users, or roles. For example, if you used the `aaa user add` command to assign a user role to a client, you can use this command to remove the role assignment. Note that you must provide either AP name or AP IP address if you want to delete bridge-mode clients.

Starting from ArubaOS 8.6.0.0, this command can be executed from the Mobility Conductor using the `ipaddr <ipaddr>` and `mac <macaddr>` parameters.

Parameter	Description
all	Deletes all connected clients.
<ip-addr>	IP address of the client to be deleted.
<ap-ip-addr>	IP address of the AP to be deleted.
ap-name	Name of the AP to be deleted.
mac <macaddr>	MAC address of the client to be deleted.
name	Name of the client to be deleted.
role	Role of the client to be deleted.

Example

To delete a user role:

```
(host) [mynode] (config) aaa user delete role web-debug
```

To delete a bridge-mode client:

```
(host) [mynode] (config) aaa user delete ap-name ap303 mac 58:94:6b:31:d0:f0
```

To delete a user from Mobility Conductor:

```
(host) [mm] (config) aaa user delete mac 58:94:6b:31:d0:f0
```

Command History

Release	Modification
ArubaOS 8.6.0.0	This command can be executed from the Mobility Conductor using the <code>ip-addr<ip-addr></code> and <code>macaddr <macaddr></code> parameters.
ArubaOS 8.2.0.0	The <code>ip-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Managed Device and Mobility Conductor

aaa user-del-req-timeout

aaa user-del-req-timeout <timeout value>

Description

This command is used to configure the user delete request timeout value. The previously entered CLI will be marked complete or timed out when the configured timeout value expires.

Parameter	Description
<timeout value>	Timeout value in minutes. Range: 1 to 30 Default: 5 minutes

Example

The following command configures the user delete request,

```
(host) [mynode] (config) #aaa user-del-req-timeout 10
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa user fast-age

aaa user fast-age

Description

This command enables fast aging of user table entries.

When this feature is enabled, if a device comes up on the network with a different IP address, the old IP address of the device is immediately deleted. If the user fast-age feature is not configured, the Mobility Conductor retains up to two IPv4 and two IPv6 addresses per device , and these IPs are aged out only when the device becomes inactive.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor executed on the managed device node.

aaa user logout

```
aaa user logout <ipaddr>
```

Description

This command logs out an authenticated client.

Parameter	Description
<ipaddr>	IP address of the authenticated client to be logged out.

Example

The following command logs out a client:

```
(host) [mynode] #aaa user logout 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa user monitor

```
aaa user monitor <ipaddr>|off
```

Description

This command checks to see whether the attributes of an authenticated user differs from those in the SOS. It also installs a timer that polls the SOS every 60 seconds and checks the following:

- ACLs
- upstream bandwidth contract
- downstream bandwidth contract

Parameter	Description
<ipaddr>	IP address of the user whose attributes are being checked.
off	Disable aaa user monitoring.

Example

The following command checks user SOS attributes:

```
(host) [mynode] (config) #aaa user monitor 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa user purge-log

aaa user purge-log

Description

This command clears aaa user log files for deleted users, it has no parameters. Per-user log files for AAA events can be used for troubleshooting issues with a specific client or device.

Example

```
(host) [mynode] (config) #aaa user purge log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

aaa user stats-poll

aaa user stats-poll <secs>

Description

This command enables user statistics polling. If enabled, ArubaOS will poll user data verify that user information in the datapath of the Mobility Conductor is in synchronization with the data in the authentication module of the Mobility Conductor.

Parameter	Description
<secs>	This command enables user statistics polling, and defines the time interval between polls. The supported range is 60-600 seconds.

Example

The following command enables user statistics polling with an interval of 10 minutes:

```
(host) ^[md] (config) aaa user stats-poll 600
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

aaa xml-api

```
aaa xml-api server <server_id>
  clone <server>
  default-authentication-role <role>
  key <key>
  no ...
```

Description

This command configures an external XML API server, which is used for authentication and subscriber management from external agents. This command configures an external XML API server. For example, an XML API server can send a blacklist/denylist request for a client to the managed device. The server configured with this command is referenced in the AAA profile for the WLAN (see [aaa profile on page 88](#)).

Parameter	Description
server	IP address of the external XML API server.
clone	Name of an existing XML API server configuration from which parameter values are copied.
default-authentication-role <role>	Name of the role to be assigned to users after completing XML server authorization.
key	Preshared key to authenticate communication between the Mobility Conductor and the XML API server.
no	Negates any configured parameter.

Example

The following configures an XML API server:

```
(host) ^[md] (config) aaa xml-api server 10.210.1.245
key qwerTYuiOP
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config mode on Mobility Conductor.

acl-debug alias-rule-hits type

```
acl-debug alias-rule-hits type
  role <name>
  route <name>
  session <name>
```

Description



- Aruba7220 Series controllers support a maximum of 8192 entries in the ACE table.
- Aruba9000 Series and Aruba7000 Series controllers support a maximum of 16384 entries in the ACE table.

Issue this command under the supervision of Aruba technical support to enable the collection and display of advanced ACL debugging information.

This command allocates hits-indices for role, route, and session ACEs expanded in an ACE with aliases.

Parameter	Description
role <name>	Name of the role for which you want to record advanced debugging information.
route <name>	Name of the route for which you want to record advanced debugging information.
session <name>	Name of the session for which you want to record advanced debugging information.

The action command `acl-debug alias-rule-hits type <acl-type> <name>` is used to allocate hits-indices for expanded-ACEs, and clear the Consolidate-Hits flag in the ACE.



Expanded-ACEs refer to the ACEs expanded in Datapath as per the netdestination usage in the ACE.



The Consolidate-Hits flag is a new flag introduced in ArubaOS 8.8.0.0 and is used to conserve the hits-indices allocation. In ArubaOS 8.7.0.0, hits-indices were allocated to all expanded-ACEs. In Aruba 8.8.0.0, the default behavior is to avoid that allocation and allow the user to allocate using the debug commands. This is a behavior change in ArubaOS 8.8.0.0 and is done to conserve the hits-indices usage.

As this is a change in the ACL, Auth will download the ACEs and ACL to Datapath. The corresponding clear command `cmd - clear acl-debug alias-rule-hits type <acl-type> <name>` will reclaim the hits-indices allocated to the ACL, and re-download the ACEs and ACLs with the Consolidated-Hits flag set.

The action command could fail when a lot ACLs are being debugged and current system limits are exceeded. In that case, a failure message indicates that the hits-indices allocation for the ACL has failed.

The action commands in the examples below are to be executed only when an ACL is being debugged.

Examples

This section illustrates an example user-role with Consolidated-Hits set by default and hits-indices allocated during debugging.

ACL Hits debugging with Consolidated-Hits Flag set (default)

```
(host) [mynode] #show acl acl-table | include sacl-allow-internal,role1
101 session 925 1 2 sacl-allow-internal 0
102 session 0 0 1 apprf-role1-sacl 0
103 role 927 3 4 role1 0
(A7210) #show acl ace-table acl 103 verbose
927: any netdest-id: 35 0 0-0 0-0 f9000080001:permit alias-dst consolidated-hits
928: any any 0 0-0 0-0 f80001:permit
929: any any 255 0-0 0-0 f100001:permit
930: any any 0 0-0 0-0 f180000:deny
<no hits-table indices are allocated>
(A7210) #show acl hits role role1
User Role ACL Hits
-----
Role Policy Src Dst Service/Application Action Dest/Opcode New Hits Total Hits
Index
Ipv4/Ipv6
-----
--
role1 sacl-allow-internal any dst-internal any permit 8 8 8607 ipv4
role1 allowall any any any permit 69 113 8608 ipv4
role1 allowall any any any-v6 permit 0 48 8609 ipv6
```

ACL Hits debugging with hits-indices allocated (debug mode)

```
(host) [mynode] #show acl ace-table acl 103 verbose
927: any netdest-id: 35 0 0-0 0-0 f1000080001:permit alias-dst hits-index: 24589
24589: any 10.1.1.41 255.255.255.255 0 0-0 0-0 f80001:permit
24590: any 10.7.0.7 255.255.255.255 0 0-0 0-0 f80001:permit
24591: any 10.9.198.121 255.255.255.255 0 0-0 0-0 f80001:permit
928: any any 0 0-0 0-0 f80001:permit
929: any any 255 0-0 0-0 f100001:permit
930: any any 0 0-0 0-0 f180000:deny
<hits-table indices are allocated>
(A7210) #show acl hits role role1
User Role ACL Hits
-----
Role Policy Src Dst Service/Application Action Dest/Opcode New Hits Total Hits
Index Ipv4/Ipv6
-----
--
role1 sacl-allow-internal any dst-internal any permit 8 8 24589 ipv4
role1 sacl-allow-internal any dst-internal any permit 6 6 24590 ipv4
role1 allowall any any any permit 69 113 8608 ipv4
role1 allowall any any any-v6 permit 0 48 8609 ipv6
```

Related Commands

Command	Description
show acl acl-table	This command shows ACL table in Auth.
show acl ace-table	This command shows ACE table in Auth.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

activate

```
activate sync
  add-only
  ca-cert <cacert>
  device-whitelist-enable / device-allowlist-enable
  device-interval <frequency>
  get-activation-key
  interval <days>
  no ...
  password <password>
  provisionurl <provisionurlname>
  sync
  url <urlname>
  username <username>
  whitelist download / allowlist download
  whitelist-enable / allowlist-enable
```

Description

This command synchronizes a managed device or a remote AP whitelist/allowlist on Mobility Conductor with the Activate whitelist/allowlist database. The Mobility Conductor and the Activate server must have layer-3 connectivity to communicate.

Parameter	Description
add-only	Allow only addition or modification of entries to the Activate remote AP whitelist/allowlist database. This parameter is enabled by default. If this setting is disabled, the activate-whitelist-download/activate-allowlist-download command can both add and remove entries from the Activate database.
ca-cert <cacert>	Use this command to manually upload self signed certificate and establish a trust relationship for a successful IPsec connection between the managed device and Activate server.
device-whitelist-enable / device-allowlist-enable	Use this command to enable managed device's whitelist/allowlist synchronization with the Activate server. This feature is disabled by default.
device-interval <frequency>	Number of hours between the automatic synchronization of the controller's whitelist/allowlist entries with the Activate server. The supported range is 1 - 168 hours.
get-activation-key	Issue this command to get activation key for the device.
interval <days>	Number of days between the automatic synchronization of the controller remote AP whitelist/allowlist entries with Activate. The supported range is 1-7 days, and the default value is 1 day.
no	Removes or disables an existing parameter.

Parameter	Description
password <password>	Activate user password.
provisionurl <provisionurlname>	Enter the URL of the page that provisions the devices to be managed by the Activate server. The default URL is https://devices.arubanetworks.com .
sync	Execute the activate sync command to immediately synchronize the list of managed devices on the Activate server with the managed device whitelist/allowlist on Mobility Conductor. By default, this list is synchronized every hour.
username <username>	Activate username.
url<urlname>	Enter the URL of the Activate server where users can provision and manage devices. The default URL is https://activate.arubanetworks.com .
whitelist download / allowlist download	Issue this command to download and synchronize Mobility Conductor's remote AP and managed device whitelist/allowlist from the Activate server.
whitelist-enable / allowlist-enable	Issue this command to enable secure remote AP and managed device whitelist/allowlist synchronization with the Activate service. This feature is disabled by default.

Example

The following example synchronizes the Activate whitelist/allowlist with the remote AP whitelist/allowlist on the controller:

```
(host) [mynode] (config) # activate whitelist download / allowlist download
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The following terminologies are updated: <ul style="list-style-type: none"> All instances of <code>master</code> have been replaced with <code>conductor</code>. All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor , except for the <code>whitelist/allowlist</code> <code>download</code> and <code>sync</code> parameters, which are available in enable mode only.

add ap arm client-match unsupported

```
add ap arm client-match unsupported <mac-addr>
```

Description

This command marks a station as unsupported by ClientMatch .

This is an internal command used to diagnose and debug ClientMatch issues, and should be used only under the supervision of customer support.

Parameter	Description
<mac-addr>	MAC address of the station to be ignored by ClientMatch.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

adp

```
adp
  discovery
  igmp-join
  igmp-vlan <igmp-vlan-id>
```

Description

This command configures the ADP. Aruba APs send out periodic multicast and broadcast queries to locate Mobility Conductor. If the APs are in the same broadcast domain as Mobility Conductor and ADP is enabled on the managed device, the managed device automatically responds to the queries of APs with its IP address. If the APs are not in the same broadcast domain as Mobility Conductor, you need to enable multicast on the network. You also need to make sure that all routers are configured to listen for IGMP join requests from the managed device and can route the multicast packets. Use the `show adp config` command to verify that ADP and IGMP join options are enabled on the managed device.

Parameter	Description
discovery	Enables or disables ADP on the managed device. enabled
igmp-join	Enables or disables sending of Internet Group Management Protocol (IGMP) join requests from a managed device. enabled
igmp-vlan	VLAN to which IGMP reports are sent. 0

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

airgroup

```
airgroup
  active-domain
  blocked-service
  cppm-server
  disallow-vlan
  dlna
  domain
  exclude-switch
  ipv6
  mdns
  policy
  send-query
  server
  server-refresh
  test-server
  version
```

Description

This command configures AirGroup settings.

Parameter	Description
<code>active-domain <string></code>	Configures active domain for AirGroup cluster. NOTE: This parameter is available only in Config mode.
<code>blocked-service</code>	Enable tracking blocked services.
<code>cppm-server</code> <code> aaa</code> <code> rfc-3576-server <rfc3576_server></code> <code> rfc3576_udp_port <rfc3576_udp_port></code> <code> server-dead-time <server-dead-time></code> <code> server-group <server-group></code> <code> query-interval <1..24></code>	Configures the following in AirGroup AAA profile: rfc-3576-server <rfc3576_server> : Configures RFC 3576 server IP address. rfc3576_udp_port <rfc3576_udp_port> : Configures UDP port number.

Parameter	Description
	<p>server-dead-time <server-deadtime>: Server dead time in minutes. To disable the server dead time, set the value to 0.</p> <p>server-group<server-group>: Name of the server group.</p> <p>NOTE: This parameter is available only in Config mode.</p>
<pre>disallow-vlan <1..4094> servers users string servers users</pre>	<p>Configures the following disallowed VLAN.</p> <p><1..4094> {servers users}: Blocks all AirGroup servers/users on this VLAN ID.</p> <p>string {servers users}: Blocks all AirGroup servers/users on this VLAN name.</p> <p>NOTE: This parameter is available only in Config mode.</p>
<pre>dlna</pre>	<p>Configures AirGroup DLNA support.</p> <p>NOTE: This parameter is available only in Config mode.</p>

Parameter	Description
<pre>domain <string> description <description> ip-address <ipaddr> no</pre>	<p>Configures AirGroup domain.</p> <p>NOTE: This parameter is only available in Config mode.</p>
<pre>exclude-switch <mac></pre>	<p>Excludes management of AirGroup on this managed device where:</p> <p><mac>: MAC address of managed device.</p> <p>NOTE: This parameter is only available in Config mode.</p>
<pre>ipv6</pre>	<p>Configures IPv6 support for AirGroup.</p> <p>NOTE: This parameter is only available in Config mode.</p>
<pre>mdns</pre>	<p>Configure AirGroup mdns support.</p> <p>NOTE: This parameter is only available in Config mode.</p>
<pre>policy ap-fqln device-mac <mac> {add <string>} {remove <string>} {string}</pre>	<p>Configures shared AP-FQLN for this server</p>
<pre>policy ap-group device-mac <mac> {add <string>} {remove <string>} {<string>}</pre>	<p>Configure shared AP-group for this server</p>

Parameter	Description
<pre>policy ap-name device-mac <mac> {add <string>} {remove <string>} {<string>}</pre>	Configure shared AP-name for this server
<pre>policy ap-neighborhood device-mac <mac> number</pre>	Consider neighborhood of configured AP names
<pre>policy autoassociate device-mac <mac> {ap-fqln} {ap-group} {ap-name}</pre>	Auto associate this wireless server with its AP-name/AP-FQLN/AP-group.
<pre>policy shared-group device-mac <mac> {add <string>} {remove <string>} {<string>}</pre>	Configure groups shared with this server
<pre>policy shared-role device-mac <mac> {add <string>} {remove <string>} {<string>}</pre>	Configure shared role-name for this server
<pre>policy shared-user device-mac <mac> {add <string>} {remove <string>} {<string>}</pre>	Configure users shared with this server
<pre>policy XX:XX:XX:XX:XX:XX</pre>	Server MAC address in XX:XX:XX:XX:XX:XX format.
<pre>send-query <client mac address> {service-id <service-id> ap-name <ap-name> vlan <vlan id> user- role <user role> user-group <user group> user-name <user name>}</pre>	Sends a query to get the list of servers that are available for a client.
<pre>server enforce-registration</pre>	<p>Configures mDNS devices to be visible only if allowed through ClearPass Policy Manager.</p> <p>NOTE: This parameter is only available in Config mode.</p>

Parameter	Description
<pre>server-refresh service <string> vlan <1..4094> <mac></pre>	<p>Sends refresh packet to refresh the cache of AirGroup server.</p> <p><service <string> vlan <1..4094>: AirGroup service.</p> <p><mac>: MAC address of AirGroup server.</p>
<pre>test-server <name> <macaddr></pre>	<p>Tests AirGroup RADIUS server.</p> <p><name>: Name of RADIUS server.</p> <p><macaddr>: MAC address of RADIUS server.</p>
<pre>version ver1 ver2</pre>	<p>Switches between AirGroup version1 (older AirGroup) and version2 (redesigned AirGroup) on the Mobility Conductor.</p> <p>NOTE: This parameter is only available on the Mobility Conductor.</p>

Example

Access the CLI and use the following command to configure AirGroup command:

```
(host) [mynode] #airgroup policy shared-group device-mac 00:1a:1e:aa:bb:cc add
test
(host) [mynode] (config) #airgroup exclude-switch 00:1a:1e:aa:bb:cc
```

Related Commands

Command	Description
show airgroup	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.11.0.0	The send-query parameter was introduced.
ArubaOS 8.8.0.0	The <code>version</code> parameter was introduced.
ArubaOS 8.1.0.0	The <code>static</code> parameter was removed.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

airgroupprofile

```
airgroupprofile
  activate {airgroupprofile <airgroup_profile> [<mode> {<centralised>| <distributed>}]}
  cppm <name>
    clone <source>
    query-interval-time <query-interval-time>
    rfc-3576-server <rfc-3576-server>
    rfc3576_udp_port <rfc3576_udp_port>
    server-dead-time <server-dead-time>
    server-group <server-group>
  no
  domain <name>
    clone <source>
    description <description>
    ip-addr <ip-addr>
  no
  ipv6 <name>
    clone <source>
  network <network-profile-name>
    blacklist-mac/denylist-mac <macaddr>
    clone
    include-domain-name
    max-ip-per-device <number of ip addresses>
    max-servers-in-location
    max-servers-per-query
    max-tokens-per-device <number of tokens>
  no
    wired-server-expiry
    wireless-server-expiry
  service <service-name>
    clone <source>
    description
    id <string>
  no
  <profile-name>
    active-domain-profile <airgroup-domain-name>
    autoassociate [apfqln|apgroup|apname]
    clone <source>
    cppm-profile <airgroup-cppm-name>
    disallow-role <role>[type{servers|users}[service]]
    disallow-vlan <vlan>[type{servers|users}[service]]
    enforce-registration
    ipv6-profile <ipv6-profile-name>
    network-profile <network-profile-name>
  no
    service <airgroup-service-name>
```

Description

This command configures an AirGroup profile.

Parameter	Description
activate airgroupprofile <airgroup_profile>	Configures the active AirGroup profile.

Parameter	Description
<pre>mode {centralised distributed}</pre>	<p>This parameter is supported only on the managed devices.</p> <ul style="list-style-type: none"> ■ airgroupprofile: Configure the AirGroup profile. ■ mode: Configure AirGroup profile in centralised or distributed mode.
<pre>cppm <name> clone <source> no query-interval-time <query-interval-time> rfc-3576-server <rfc-3576-server> rfc3576_udp_port <rfc3576_udp_port> server-dead-time <server-dead-time> server-group <server-group></pre>	<p>Configures an AirGroup ClearPass Policy Manager profile.</p> <ul style="list-style-type: none"> ■ clone: Copy profile data from another AirGroup profile. ■ no: Delete the command. ■ query-interval-time: Specify the time interval, in seconds, between general queries. ■ rfc-3576-server: Configure RFC 3576 server IP address. ■ rfc3576_udp_port: Configure UDP port number. ■ server-dead-time: Configure the server dead time, in minutes. To disable the server dead time, set the value to 0. The default value is 10 minutes. ■ server-group: Configure the name of the server group. <p>This parameter is supported only on the managed devices.</p>
<pre>domain <name> clone <source> description <description> ip-addr <ip-addr> no</pre>	<p>Configures an AirGroup domain profile.</p> <ul style="list-style-type: none"> ■ clone: Copy domain profile data from another AirGroup profile. ■ description: Configure the domain name description. ■ ip-addr: Configure the IP address of the controller. ■ no: Delete the command. <p>This parameter is supported only on the managed devices.</p>
<pre>ipv6 <name> clone <source></pre>	<p>Configures an AirGroup IPv6 profile.</p> <p>clone: Copy IPv6 profile data from another AirGroup profile.</p> <p>This parameter is supported only on the managed devices.</p>
<pre>network <network-profile-name> blacklist-mac/denylist-mac <macaddr> clone include-domain-name max-ip-per-device <number of ip addresses> max-servers-in-location max-servers-per-query max-tokens-per-device <number of tokens> no wired-server-expiry wireless-server-expiry</pre>	<p>Configures the network profile.</p> <ul style="list-style-type: none"> ■ blacklist-mac/denylist-mac: Blocks the client or server based on the MAC address or MAC OUI. ■ clone: Copy data from another Network profile. ■ include-domain-name: Includes the domain name for username based policies. <ul style="list-style-type: none"> ■ Default: disabled ■ max-ip-per-device: Limits the

Parameter	Description
	<p>number of maximum allowed IP addresses per server.</p> <ul style="list-style-type: none"> ■ Default: 4 ■ Range: 1 to 64 ■ max-servers-in-location: Limits the maximum number of servers in location. ■ Default: 100 ■ max-servers-per-query: Limits the maximum number of servers per query . ■ Default: 30 ■ max-tokens-per-device: Limits the number of maximum tokens allowed per server or client. ■ Default: 40 ■ Range: 1 to 64 ■ no: Delete the command. ■ wired-server-expiry: Specify expiry time for wired servers in minutes. ■ Default: 10 ■ wireless-server-expiry: Specify expiry time for wireless servers in minutes. ■ Default: 120 <p>This parameter has the following limitations:</p> <ul style="list-style-type: none"> ■ User defined network-profile is not supported. ■ The default network-profile is always enabled and cannot be disabled when any airgroupprofile is activated. ■ The default network-profile can be modified only from /md hierarchy node. ■ In case of multiple islands, the network-profile is activated only to the island where the airgroupprofile is activated.
<pre> service <service-name> clone <source> description <service_desc> id <service_id> no </pre>	<p>Configures an AirGroup service profile. By default, the following services are available:</p> <ul style="list-style-type: none"> ■ custom ■ default-airplay ■ default-airprint ■ default-allowall ■ default-amazontv ■ default-dial ■ default-dlna-media ■ default-dlna-print ■ default-googlecast ■ default-itunes ■ default-remotemgmt ■ default-sharing <p>■ DIAL</p>

Parameter	Description
	<p>Clone: Copy service profile data from another AirGroup service profile.</p> <p>Description: Description of AirGroup service profile.</p> <p>ID: Identity of AirGroup service profile.</p> <p>No: Disable AirGroup service profile. This parameter is supported only on the managed devices.</p>
<pre> <profile-name> active-domain-profile <airgroup-domain-name> autoassociate {apfqln apgroup apname} clone <source> cppm-profile <airgroup-cppm-name> disallow-role <role>[type{servers users}[service]] disallow-vlan <vlan>[type{servers users}[service]] enforce-registration ipv6-profile <ipv6-profile-name> network-profile <network-profile-name> service <airgroup-service-name> no </pre>	<p>Configures an AirGroup profile.</p> <ul style="list-style-type: none"> ■ active-domain-profile: Configure an AirGroup domain profile. ■ autoassociate: Auto associate servers with the AirGroup profile. Use the following sub-parameters: <ul style="list-style-type: none"> ■ apfqln: Auto associate with AP FQLN. ■ apgroup: Auto associate with AP Group. ■ apname: Auto associate with AP Name. ■ clone: Copy profile data from another AirGroup profile. ■ cppm-profile: Configure CPPM profile for the AirGroup profile. ■ disallow-role: Configure disallowed roles with AirGroup profile. ■ disallow-vlan: Configure disallowed vlans with AirGroup profile. ■ enforce-registration: Enforce server registration with AirGroup profile. ■ ipv6-profile: Configure an IPv6 profile with AirGroup profile. ■ network-profile: Configure AirGroup Network profile with AirGroup profile. ■ service: Configure AirGroup service profile name. <p>This parameter is supported only on the managed devices.</p>

Example

Access the CLI and use the following command to configure an AirGroup profile for the DIAL service:

```

(host) [md] (config) #airgroupprofile service DIAL
(host) [md] (Airgroup Service Profile "DIAL") #description This is the
DIAL service

```

The following example configures the network default parameter:

```

host) [md] (config) #airgroupprofile network default
(host) [md] (Network profile "default") #blacklist-mac/denylist-mac <macaddr>
(host) [md] (Network profile "default") #max-ip-per-device <number of ip
addresses>
(host) [md] (Network profile "default") #max-tokens-per-device <number of tokens>

```

Related Commands

Command	Description
show airgroupprofile	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.11.0.0.0	The include-domain-name sub-parameter was added to the network default parameter.
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.6.0.3	The <code>network default</code> parameter was introduced.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

airmatch ap

```
airmatch ap freeze all-aps|[ap-group <ap-group>]|[ap-name <ap-name>]|[ip-addr <ip-addr>]|  
[ip6-addr <i6p-addr>] [band <band>] | [channel <channel>]| [eirp <dBm>]| [lms lms-ip  
<lms-ip>] | [lms-ipv6 <lms-ipv6>]
```

```
airmatch ap unfreeze all-aps|[ap-group <ap-group>]|[ap-name <ap-name>]|[ip-addr <ip-  
addr>]|[ip6-addr <i6p-addr>] band <band> | [channel <channel>]| [eirp <dBm>]| [lms lms-ip  
<lms-ip>] | [lms-ipv6 <lms-ipv6>]
```

Description

The `airmatch ap freeze` command deploys the specified channel and EIRP values to a radio immediately, then freezes those values, regardless of whether the AirMatch RF planning schedule is enabled or disabled. A radio set with the `airmatch ap freeze` command uses a static radio configuration until those settings get explicitly canceled with the `airmatch ap unfreeze` command. This command can be used to freeze either the channel or the EIRP value, or both values. For example, you can freeze the channel on an AP radio, while allowing the EIRP values to be updated by AirMatch.

Syntax

Parameter	Description
<code>freeze</code>	Apply the specified AirMatch settings on the radio, then freeze those settings until they are manually removed. This parameter supports both single radio and dual-radio APs.
<code>unfreeze</code>	Remove AirMatch settings manually applied using the Freeze command. This parameter supports both single radio and dual-radio APs.
<code>all-aps</code>	Freeze or unfreeze AirMatch settings on all APs.
<code>ap-group <ap-group></code>	Freeze or unfreeze AirMatch settings on the specified AP group
<code>ap-name <ap-name></code>	Freeze or unfreeze AirMatch settings on the specified AP
<code>ip-addr <ip-addr></code>	Freeze or unfreeze AirMatch settings on the AP with the specified IPv4 IP address.
<code>ip6-addr <i6p-addr></code>	Freeze or unfreeze AirMatch settings on the AP with the specified IPv6 IP address.
<code>band <band></code>	Set AirMatch settings for the specified radio band. Supported values are 2.4GHz and 5GHz . The radio band <i>must</i> be specified if you use the unfreeze parameter to unfreeze an AP radio. The values, 5GHzu for upper-band radios and 5GHzl for lower-band radios are supported by the following APs. <ul style="list-style-type: none">■ AP-344■ AP-345■ AP-555

Parameter	Description
channel <channel>	Channel number for the AP 802.11a/b/g, 802.11n or 802.11ac physical layer, (example: 1, 1+, 36, 36+, 36E, 36S, 36E+149E). The available channels depend on the regulatory domain (country). <ul style="list-style-type: none"> ■ 36S is 160 MHz wide contiguous channel ■ 36E+149E is 160 MHz wide channel defined as 2 separate 80 MHz channel ranges
eirp <dBm>	The transmission power level (in dBm) to be assigned to the AP radio(s). Starting with ArubaOS 8.2, you can specify EIRP values in increments of .1 dBm. 270 Series access points support both positive and negative EIRP values. All other APs support positive EIRP values only. The following legacy APs do <i>not</i> support advanced power controls, and can only be configured in positive EIRP values in increments of .5 dBm. <ul style="list-style-type: none"> ■ 90 Series ■ 100 Series ■ 110 Series ■ 170 Series ■ RAP-155
lms lms-ip <lms-ip> lms-ipv6 <lms-ipv6>	Include this parameter to freeze or unfreeze AP channels on a local controller. This parameter is only valid if you freeze or unfreeze channels using the ap-group or all-aps options.

Example

```
(host)[mynode](config)# airmatch ap freeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{ap-name <ap-name>}|{ap-group <ap-group>}|{all-aps} {band <band>}|{channel <channel>}|{eirp <eirp>}|lms {lms-ip <lms-ip>}|{lms-ipv6 <lms-ipv6>}}
```

Unfreezing a radio configuration with the `airmatch ap unfreeze` command does not mean that there will automatically be an immediate change in the channel and EIRP values for that radio. It does, however, mean that the AirMatch algorithm can assign a new set of values at the next update.

```
(host)[mynode](config)# airmatch ap unfreeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{ap-name <ap-name>}|{ap-group <ap-group>}|{all-aps} band <band> {channel <channel>}|{eirp <eirp>}|lms {lms-ip <lms-ip>}|{lms-ipv6 <lms-ipv6>}}
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.6.0.0	The values, 5GHzu for upper-band radios and 5GHzl for lower-band radios are supported by AP-555 access points.
ArubaOS 8.3.0.0	The <code>freeze</code> and <code>unfreeze</code> parameters support dual 5 GHz radio APs.
ArubaOS 8.2.0.0	The <code>eirp</code> parameter supports the configuration of EIRP values in .1 dBm increments. EIRP values for 270 Series access points can be configured as a negative value.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Mobility Conductor	Base operating system.	Config mode on Mobility Conductor.

airmatch ap-partition

```
airmatch ap-partition start <cluster-name>
```

Description

This command will start AP partitioning for a specific cluster.

Parameter	Description
start <cluster-name>	Start partitioning of the APs for the specified cluster name.

Example

```
(host) [mynode] #airmatch ap-partition start test
AP Partitioning starts for cluster test.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

airmatch db-dump

```
airmatch db-dump  
all  
collection
```

Description

This command creates a dump of the database used by AirMatch. The dump file can be exported using the **copy** command.

Parameter	Description
all	Create a dump file of the entire AirMatch database
collection <collection>	Create a dump file of a specific collection of AirMatch files by specifying the name of a collection type.

Example

The following command creates a dump file of the collection of AirMatch AMON statistics.

```
(host)[mynode]# airmatch db-dump all
```

Related Commands

Command	Description
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.
airmatch profile	This command configures the AirMatch profile.
airmatch runnow	Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
Mobility Conductor	Base operating system.	Enable mode on Mobility Conductor.

airmatch profile

```
airmatch profile
  he-pooling-client-density <he-pooling-client-density>
  dfs-ch-deploy-interval
  deploy-hour <0-23>
  no ...
  noise-event-period-2g <noise-event-period-2g>
  noise-event-period-5g <noise-event-period-5g>
  quality-threshold <quality-threshold>
  quality-threshold-2-4GHz
  quality-threshold-5GHz
  quality-threshold-6GHz
  radar-event-period-5g <radar-event-period-5g>
  schedule enable|disable
  solver-feas-deploy-threshold <solver-feas-deploy-threshold>
  use-intf-device
```

Description

This command configures the AirMatch profile.

The AirMatch channel and EIRP optimization features deprecate the channel planning and EIRP optimization features in the legacy ARM feature. AirMatch is supported on Mobility Conductor only, while legacy ARM channel optimization and EIRP features continue to be supported by stand-alone controllers running ArubaOS 8.x.

AirMatch channel planning evens out channel distributions in any size of network, and in any subset of the contiguous network (as much as allowed by the network configuration, regulatory domain and AP hardware capability). AirMatch also minimizes channel coupling, where adjacent radios are assigned to the same channel. The computing power of Mobility Conductor impacts channel distribution calculations, so channel coupling may occasionally be allowed in complex networks to keep the computing time practical.

AirMatch EIRP planning automatically considers the local density of the network to manage the APs' coverage and modulation and coding scheme (MCS) operation, and optimizes EIRP changes across neighboring AP radios in order to offer users the best roaming experience.

The AirMatch **schedule disable** setting is different from the ARM setting of **disable** or **maintain**. The ARM **disable** setting changes the AP radio channel and EIRP values back to the default values specified in 802.11a and 802.11g radio profiles for that radio. The ARM **maintain** setting freezes current channel and EIRP settings for that radio. In contrast, the AirMatch **schedule disable** option simply means the centralized algorithm will stop selecting a new channel, bandwidth, or EIRP setting; the network operator still can override the previous settings assigned by AirMatch with static channel or EIRP values, and the AP radio can continue to voluntarily change channels to avoid radar interference or high noise levels.

AirMatch Channel Assignments

Each AP in a Mobility Conductor deployment measures its RF environment for a five minute period, every 30 minutes, by default. The AP then sends AMON messages about the radio feasibility to the managed device based on the hardware capability for the AP, radio and regulatory domain, and RF neighbors. The managed device forwards these messages to the Mobility Conductor. The Mobility Conductor adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs. By default, this configuration update is sent at 5 AM (as per

the Mobility Conductor system clock), but time of this configuration update can be modified via the AirMatch profile.

An exception to this daily update is an automatic channel change due to a radar detection event or high noise interference. If an AP detects a radar event on its current operating channel, that AP automatically changes to another supported channel to avoid radar interference, and does not wait for the daily RF configuration update from the Mobility Conductor. An AP may also automatically change channels if a very high noise level is detected on the current channel, if at least one other channel is free of noise.

In ArubaOS 8.0, AirMatch moves a radio to a random channel when a radar event is detected, or if a high noise floor is detected on a non-static channel. Starting with ArubaOS 8.0.1, AirMatch uses the criteria described in [Table 6](#) to assign a new channel.

Table 6: Channel Assignment Logic

Issue Prompting Channel Change	Channel Selection Criteria
Detected radar	AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.
High channel noise	<p>The channel selection criteria varies between static and non-static channels.</p> <ul style="list-style-type: none"> ■ If static channel is configured, the channel does not change due to a high noise condition. ■ For a non-static channel, AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.

Channel Quality Improvement Thresholds

ArubaOS 8.0.1 introduces the AirMatch channel quality improvement threshold, which allows you to select the minimum channel improvement that can trigger a new scheduled channel solution. The default threshold value is a 15% improvement. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.

EIRP settings are not impacted by the channel quality improvement threshold. A new EIRP plan is deployed at the scheduled deployment hour every day, regardless of channel quality improvement levels.

This channel quality setting only applies to scheduled updates. If you manually trigger an update using the `airmatch runnow` command, AirMatch will deploy the new solution regardless of the level of improvement.

Parameter	Description
deploy-hour <0-23>	<p>Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device. If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.</p> <p>0-23 5</p>

Parameter	Description
he-pooling-client-density <he-pooling-client-density>	Specify a HE pooling client density in percentage to be considered for 802.11ax pooling. Va HE pooling client density of 0 disables HE pooling. 0-100 20
dfs-ch-deploy-interval	Configures the time interval (in minutes) between the deployment of radios assigned to operate on DFS channels. 0,1 0
no ...	Negates any configured parameter
noise-event-period-2g <noise-event-period-2g>	Use this advanced configuration parameter under the supervision of Aruba support only.
noise-event-period-5g <noise-event-period-5g>	Use this advanced configuration parameter under the supervision of Aruba support only.
quality-threshold <quality-threshold>	Use the <code>quality-threshold</code> parameter to change the percentage of channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change. This setting only applies to scheduled updates. If you manually trigger an update using the <code>airmatch runnow</code> command, AirMatch will deploy the new solution regardless of the level of improvement. If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved by greater than this threshold value. A new EIRP plan is deployed on the deployment hour every day. 0-100 8
quality-threshold-2-4GHz	Use the <code>quality-threshold-2-4GHz</code> parameter to change the percentage of 2.4 GHz channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change. This setting only applies to scheduled updates. If you manually trigger an update using the <code>airmatch runnow</code> command, AirMatch will deploy the new solution regardless of the level of improvement. If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved by greater than this threshold value for 2.4 Ghz radio. A new EIRP plan is deployed on the deployment hour every day. 0-100 8

Parameter	Description
quality-threshold-5GHz	<p>Use the <code>quality-threshold-5GHz</code> parameter to change the percentage of 5 GHz channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.</p> <p>This setting only applies to scheduled updates. If you manually trigger an update using the <code>airmatch runnow</code> command, AirMatch will deploy the new solution regardless of the level of improvement.</p> <p>If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved by greater than this threshold value for 2.4 Ghz radio. A new EIRP plan is deployed on the deployment hour every day.</p> <p>0-100 8</p>
quality-threshold-6GHz	<p>Use the <code>quality-threshold-6GHz</code> parameter to change the percentage of 6 GHz channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.</p> <p>This setting only applies to scheduled updates. If you manually trigger an update using the <code>airmatch runnow</code> command, AirMatch will deploy the new solution regardless of the level of improvement.</p> <p>If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved by greater than this threshold value for 2.4 Ghz radio. A new EIRP plan is deployed on the deployment hour every day.</p> <p>0-100 8</p>
radar-event-period-5g <radar-event-period-5g>	<p>Use this advanced configuration parameter under the supervision of Aruba support only.</p>
schedule enabled disabled	<p>If the AirMatch schedule updates are changed from the default enabled setting to disabled, the Mobility Conductor continues to receive RF updates from the APs, but no channel and EIRP changes are executed by Mobility Conductor at the scheduled time.</p> <p>When AirMatch schedules are disabled, the centralized algorithm stops selecting a new channel, bandwidth, stops EIRP setting. A network operator still can override the previous settings assigned by AirMatch with static channel or EIRP values, and the AP radio can continue to voluntarily change channels to avoid radar interference or high noise levels.</p> <p>enabled</p>
solver-feas-deploy-threshold <solver-feas-deploy-threshold>	<p>Use this advanced configuration parameter under the supervision of Aruba support only.</p>
use-intf-device	<p>Enable this configuration to include interferer in the RF-domain and partition computation .</p> <p>Disabled</p>

Parameter	Description
	CAUTION: Enabling this parameter will highly impact AirMatch solution.

Example

To hold the existing AirMatch RF configuration :

```
(host) [mynode] (config) # airmatch profile schedule disabled
```

To change the time of the daily AirMatch RF updates from the default 5 AM to 2 AM:

```
(host) [mynode] (config) # airmatch profile deploy-hour 2
```

Related Commands

Command	Description
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.
airmatch db-dump	This command creates a dump of the database used by AirMatch. The dump file can be exported using the <code>copy</code> command.
airmatch runnow	Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.
show airmatch profile	This command displays the configuration settings in the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The dfs-ch-deploy-interval parameter was introduced.
ArubaOS 8.7.0.0	The <code>he-pooling-client-density</code> parameter was introduced.
ArubaOS 8.2.1.0	The default value of the <code>quality-threshold</code> parameter was changed to 8%.
ArubaOS 8.1.0.0	The <code>eirp-offset</code> parameter was removed from this command, and was introduced in rf dot11a-radio-profile and rf dot11g-radio-profile commands.

Release	Modification
ArubaOS 8.0.1.0	The <code>quality-threshold</code> parameter was added.
ArubaOS 8.0.0.0	This command was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

airmatch runnow

```
airmatch runnow
  eirp
  full
  incremental
  opmode
  quick
```

Description

Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.

Parameter	Description
<code>eirp</code>	Initiates only the EIRP optimization.
<code>full</code>	Initiate the process to perform a full optimization of all APs.
<code>incremental</code>	Optimize only the new APs that have never been optimized by a previous AirMatch solution.
<code>opmode</code>	Generate an AirMatch solution with an opmode update.
<code>quick</code>	Quickly generate an AirMatch solution. This option may produce an AirMatch solution that is not as optimal as a full or regularly-scheduled optimization.

Example

To initiate a full optimization of all APs, access the Mobility Conductor CLI in enable mode and issue the following command:

```
(host)[mynode] #airmatch runnow full
```

Related Commands

Command	Description
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.
airmatch profile	This command configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.3.0.0	The following parameters were introduced: <ul style="list-style-type: none"> ■ eirp ■ opmode
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

airslice

```
airslice-profile <profile-name>
  airslice-app-monitoring
  airslice-policy
  clone
  no
airslice-visibility
  record-limit <record-count>
  record-limit unlimited
```

Description

This command configures or modifies an Air Slice profile.

Parameter	Description
airslice-profile <profile-name>	Configure the Air Slice profile.
airslice-app-monitoring	Enables traffic monitoring for applications.
airslice-policy	Optimizes the community quality of applications.
clone	Copies data from another Air Slice profile.
no	Deletes the profile.
airslice-visibility	Configure the Air-Slice visibility module.
record-limit <record-count>	Specify the maximum number of records to be stored for clients.
record-limit unlimited	No limit on the number of records to be stored for clients. All records are stored.

Example

The following command configures an Air Slice profile:

```
(host) [mynode] (config) #airslice-profile <name>
(host) [mynode] (airslice profile <name>) airslice-app-monitoring
(host) [mynode] (airslice profile <name>) airslice-policy
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Air Slice is supported on all 802.11ax APs. However, Air Slice is supported only on 5 GHz radio and not on 6 GHz radio for 630 Series access points.	Base operating system.	Config mode on Mobility Conductor.

ale-configuration

```
ale-configuration
  ale_sta_associated
  anonymize
  ip <ip-addr> username <uname> password <passwd>
  nbapi_publish
```

Description

Use this command to enable ALE configuration. After ALE is enabled, you can configure ALE anonymize, STA channel, IP address, and NB API.

Parameter	Description
ale_sta_associated	Publish ALE_STA channel for associated clients only.
anonymize	Station Mac Anonymization.
ip	VLAN to which IGMP reports are sent.
nbapi_publish	Enable publishing of data available via zmq, including station, virtual AP, AP, radio, RSSI, visibility_rec, destination, application; and REST API including details about floor, campus, building, Virtual AP, AP, station, radio.
no	Disable ALE on the Mobility Conductor.

Example

To enable ALE configuration:

```
(host) [mynode] (config) #ale-configuration
```

To enable anonymize in ALE:

```
(host) [mynode] (config) #ale-configuration
(host) [mynode] (config-submode) #anonymize
```

Related Commands

Command	Description
show ale-configuration	This command displays ALE configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db cpsec add / allowlist-db cpsec add

```
whitelist-db cpsec add / allowlist-db cpsec add
mac-address <name>
  ap-group <ap_group>
  ap-name <ap_name>
  description <description>
```

Description

This command adds an AP entry to the campus AP whitelist/allowlist.

You can manually add entries to the campus AP whitelist/allowlist to grant valid APs secure access to the network.

Parameter	Description
mac-address <name>	MAC address of the AP you want to enter into the campus AP whitelist/allowlist database.
ap-group <ap_group>	(Optional) Name of the AP group. If the AP group is not entered, a campus AP boots with "default" as AP group.
ap-name <ap_name>	(Optional) Name of the AP. If the AP name is not entered, a campus AP boots with its MAC address as AP name.
description <description>	(Optional) Brief description of the AP. If the description includes spaces, enclose the description in quotation marks.

Example

The following example creates a new campus AP whitelist/allowlist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host) #whitelist-db cpsec add mac-address 00:16:CF:AF:3E:E1 / allowlist-db
cpsec add mac-address 00:16:CF:AF:3E:E1
ap-group default
ap-name AP-225
description "AP-225 in lobby"
```

Related Command

Command	Description
show whitelist-db cpsec/show allowlist-db cpsec	Show the campus AP whitelist/allowlist for the control plane feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db cpsec del / allowlist-db cpsec del

```
whitelist-db cpsec del / allowlist-db cpsec del mac-address <mac-address>
```

Description

This command removes individual whitelist/allowlist entries for an AP that has been either removed from the network, or is no longer a candidate for automatic certificate provisioning. If the AP whose entry you deleted is still connected to the network and the control plane security feature is configured to send certificates to all APs (or a range of addresses that include that AP), then the managed device will send the AP another certificate, and the AP will reappear in the campus whitelist/allowlist.

Parameter	Description
<code>mac-address <mac-address></code>	MAC address of the AP you want to remove from the campus AP whitelist/allowlist.

Example

The following example removes an AP with the MAC address 10:14:CA:AF:3E:E1 from the campus AP whitelist/allowlist:

```
(host) [mynode] (config) #whitelist-db cpsec del mac-address  
10:14:CA:AF:3E:E1/allowlist-db cpsec del mac-address 10:14:CA:AF:3E:E1
```

Related Commands

Command	Description
show whitelist-db cpsec/show allowlist-db cpsec	Show the campus AP whitelist/allowlist for the control plane feature.
whitelist-db cpsec revoke / allowlist-db cpsec revoke	Revoke a certificate from an invalid or suspected rogue AP in the campus AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db cpsec modify / allowlist-db cpsec modify

```
whitelist-db cpsec modify / allowlist-db cpsec modify
  mac-address <name>
  ap-group <ap_group>
  ap-name <ap_name>
  cert-type {factory-cert|switch-cert}
  description <description>
  mode {disable|enable}
  revoke-text <revoke-text>
  state {approved-ready-for-cert|certified-factory-cert}
```

Description

This command modifies an existing entry in the campus AP whitelist/allowlist.

Parameter	Description
mac-address <name>	MAC address of an AP in the campus AP whitelist/allowlist database.
ap-group <ap_group>	(Optional) Name of the AP group to which an AP is assigned. If AP group is not entered, a campus AP boots with "default" as the AP group.
ap-name <ap_name>	(Optional) Name of an AP. If AP name is not entered, a campus AP boots with its MAC address as the AP name.
cert-type {factory-cert switch-cert}	(Optional) Type of certificate used by an AP. <ul style="list-style-type: none">■ factory-cert: AP uses a factory-installed certificate.■ switch-cert: AP uses a controller-signed certificate.
description <description>	(Optional) Brief description of an AP. If the description includes spaces, enclose the description in quotation marks.
mode {disable enable}	(Optional) Mode of an AP. <ul style="list-style-type: none">■ disable: Disables an AP in the campus AP whitelist. A disabled AP cannot contact a managed device over a secure connection.■ enable: Enables a disabled AP in the campus AP whitelist/allowlist.
revoke-text <revoke-text>	(Optional) Brief description why an AP was revoked.
state {approved-ready-for-cert certified-factory-cert}	(Optional) State of an AP. <ul style="list-style-type: none">■ approved-ready-for-cert: AP is approved and is ready to receive a certificate.■ certified-factory-cert: AP is certified and has a factory-installed certificate.

Example

The following example changes the AP group, AP name, certificate type, description, mode, revoke text, and state of an AP with MAC address 00:1E:37:CB:D4:52:

```
(host)[node] #whitelist-db cpsec modify mac-address 00:1E:37:CB:D4:52/  
allowlist-db cpsec modify mac-address 00:1E:37:CB:D4:52  
    ap-group default  
    ap-name ap-225  
    cert-type factory-cert  
    description "AP-225 in lobby"  
    mode disable  
    revoke-text "Maintenance"  
    state approved-ready-for-cert
```

Related Command

Command	Description
show whitelist-db cpsec/show allowlist-db cpsec	Show the campus AP whitelist/allowlist for the control plane feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db cpsec purge / allowlist-db cpsec purge

whitelist-db cpsec purge / allowlist-db cpsec purge

Description

This command clears all entries in the campus AP whitelist/allowlist.

If your network includes both Mobility Conductor and managed devices, then each campus AP whitelist/allowlist is synchronized across all managed devices. If you purge the entire list on one managed device, that action will clear the campus AP whitelist/allowlist on every managed device in the network. To delete an individual entry, use the command [whitelist-db cpsec del / allowlist-db cpsec del](#).

Example

The following example removes all APs from the campus AP whitelist/allowlist:

```
(host)[node] (config) #whitelist-db cpsec purge/allowlist-db cpsec purge
```

Related Command

Command	Description
show whitelist-db cpsec/show allowlist-db cpsec	Show the campus AP whitelist/allowlist for the control plane feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor/Mobility Conductor.

whitelist-db cpsec revoke / allowlist-db cpsec revoke

```
whitelist-db cpsec revoke / allowlist-db cpsec revoke mac-address <mac-address>  
revoke-text <revoke-text>
```

Description

This command revokes a certificate from an AP in the campus AP whitelist/allowlist. Use this command to revoke a certificate from a invalid or suspected rogue AP.

Parameter	Description
mac-address <mac-address>	MAC address of the AP you want to remove from the cpsec whitelist/allowlist database.
revoke-text <revoke-text>	A brief description why the AP's certificate was revoked, up to 64 alphanumeric characters. If this comment includes spaces, you must enclose the comment in quotation marks.

Example

The following example revokes a certificate from an AP. This command does not delete a whitelist/allowlist entry for a revoked AP, but marks its entry with the revoked state.

```
(host)[node] (config) #whitelist-db cpsec revoke mac-address  
00:1E:37:CA:D4:51 / allowlist-db cpsec revoke mac-address 00:1E:37:CA:D4:51  
revoke-text "revoking cert from a rogue AP."
```

Related Command

Command	Description
show whitelist-db cpsec/show allowlist-db cpsec	Show the campus AP whitelist/allowlist for the control plane feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap add /allowlist-db rap add

```
whitelist-db rap add /allowlist-db rap add mac-addr <mac-address>
  ap-group <ap-group>
  ap-name <ap-name>
  description <description>
  full-name <full-name>
  mode enable|disable
  remote-ip <ip-addr>
```

Description

This command adds an AP entry to the Remote AP whitelist/allowlist. You can manually add entries to the remote AP whitelist/allowlist to grant valid Remote APs secure access to the network.

Parameter	Description
mac-address <mac-address>	MAC address of the AP you want to enter into the remote AP whitelist/allowlist database.
ap-group <ap-group>	AP group of the remote AP.
ap-name <ap-name>	Name of the Remote AP.
description <description>	Description of the remote AP. If the description includes spaces, it must be enclosed within quotation marks.
full-name <full-name>	Name of the client using the remote AP.
remote-ip <ip-addr>	IP address used to assign a static inner IP address for the remote AP.

Example

The following example creates a new Remote AP whitelist/allowlist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node](config) #whitelist-db rap add mac-address 00:16:CF:AF:3E:E1 /
allowlist-db rap add mac-address 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description
show whitelist-db rap / show allowlist-db rap	View detailed information for the remote AP whitelist/allowlist database.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap del / allowlist-db rap del

```
whitelist-db rap del / allowlist-db rap del mac-addr <mac-address>
```

Description

This command removes an AP entry from the Remote AP whitelist/allowlist.

You can manually remove entries from the Remote AP whitelist/allowlist to revoke a Remote AP's secure access to the network.

Parameter	Description
<code>mac-address <mac-address></code>	MAC address of the AP you want to remove from the remote AP whitelist/allowlist database.

Example

The following example revokes and deletes a Remote AP whitelist/allowlist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node] (config) #whitelist-db rap del mac-address 00:16:CF:AF:3E:E1 /  
allowlist-db rap del mac-address 00:16:CF:AF:3E:E1
```

Related Command

Command	Description
whitelist-db rap add /allowlist-db rap add	Add an entry into the remote AP whitelist/allowlist.
whitelist-db rap revoke/allowlist-db rap revoke	Revoke an AP's access without removing the entry from the whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap modify / allowlist-db rap modify

```
whitelist-db rap modify / allowlist-db rap modify mac-addr <mac-address>
  ap-group <ap-group>
  ap-name <ap-name>
  description <description>
  full-name <full-name>
  mode enable|disable
  remote-ip <ip-addr>
  remote-ipv6 <ipv6-addr>
```

Description

This command removes an AP entry from the Remote AP whitelist/allowlist.

You can manually remove entries from the Remote AP whitelist/allowlist to revoke a Remote AP's secure access to the network.

Parameter	Description
mac-address <mac-address>	MAC address of the remote AP whose whitelist/allowlist database entry you want to modify.
ap-group <ap-group>	AP group of the remote AP.
ap-name <ap-name>	Name of the Remote AP.
description <description>	Description of the remote AP. If the description includes spaces, it must be enclosed within quotation marks.
full-name <full-name>	Name of the client using the remote AP.
mode enable disable	Enable or disable the remote AP without deleting it from the database.
remote-ip <ip-addr>	IPv4 address used to assign a static inner IP address for the remote AP.
remote-ipv6 <ipv6-addr>	IPv6 address used to assign a static inner IP address for the remote AP.

Example

The following example modifies a Remote AP whitelist/allowlist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node] (config) #whitelist-db rap modify mac-address 00:16:CF:AF:3E:E1
/ allowlist-db rap modify mac-address 00:16:CF:AF:3E:E1
description "AP moved to second floor"
```

Related Command

Command	Description
whitelist-db rap add /allowlist-db rap add	Add an entry into the Remote AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap purge / allowlist-db rap purge

whitelist-db rap purge / allowlist-db rap purge

Description

This command clears all entries in the entire Remote AP whitelist/allowlist.

If your network includes both Mobility Conductor and managed devices, then each Remote AP whitelist/allowlist is synchronized across all managed devices. If you purge the entire Remote AP whitelist/allowlist on one managed device, that action will clear the Remote AP whitelist/allowlist on every managed device in the network.

Example

The following example removes all APs from the Remote AP whitelist/allowlist:

```
(host)[node] (config) #whitelist-db rap purge/allowlist-db rap purge
```

Related Commands

Command	Description
whitelist-db rap del / allowlist-db rap del	Delete an individual entry in the Remote AP whitelist/allowlist.
show whitelist-db rap / show allowlist-db rap	Show the remote AP whitelist/allowlist for the control plane feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap revoke/allowlist-db rap revoke

```
whitelist-db rap revoke/allowlist-db rap revoke mac-address <mac-address> revoke-  
comment <comment>
```

Description

This command revokes a certificate from an AP in the Remote AP whitelist/allowlist . Use this command to revoke a certificate from a invalid or suspected rogue AP.

Parameter	Description
mac-address <mac-address>	MAC address of the AP you want to remove from the remote AP whitelist/allowlist database.
revoke-comment <comment>	A brief description why the AP's certificate was revoked, up to 64 alphanumeric characters. If this comment includes spaces, you must enclose the comment in quotation marks.

Example

The following example revokes a certificate from an AP. This command does not delete a whitelist/allowlist entry for a revoked AP, but marks its entry with the revoked state.

```
(host) (config) #whitelist-db rap revoke mac-address 00:1E:37:CA:D4:51 /  
allowlist-db rap revoke mac-address 00:1E:37:CA:D4:51  
revoke-comment "revoking cert from a rogue RAP."
```

Related Command

Command	Description
whitelist-db rap del / allowlist-db rap del	Delete an entry from the Remote AP whitelist/allowlist .

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap-local-switch-list/allowlist-db rap-local-switch-list

```
whitelist-db rap-local-switch-list/allowlist-db rap-local-switch-list
  del mac-addr <mac-address>
  purge
```

Description

This command deletes a managed device from the local switch table used by the Remote AP whitelist/allowlist.

If your deployment includes Mobility Conductor and managed devices, then the remote AP whitelist/allowlist on each managed device contains an entry for every remote AP on the network, regardless of the managed device to which it is connected. Mobility Conductor also maintains a whitelist/allowlist managed devices with remote AP. When you change a remote AP whitelist/allowlist on any managed device, that managed device contacts Mobility Conductor to check the local switch whitelist/allowlist, then contacts every other managed device on the local switch whitelist/allowlist to notify it of the change.

If you ever remove a managed device from the network, you must also remove the managed device from the local switch whitelist/allowlist. If the local switch whitelist/allowlist contains entries for managed devices no longer on the network, then a remote AP whitelist/allowlist entry can be marked for deletion but will not be physically deleted, as the managed device will be waiting for an acknowledgment from another managed device no longer on the network. Any unused managed device entries in the local switch whitelist/allowlist can significantly increase network traffic and reduce memory resources.

Parameter	Description
<code>del mac-address <mac-address></code>	Remove a single managed device from the local switch table.
<code>purge</code>	Clear all managed devices from the local switch table

Example

The following example removes a managed device from the local switch whitelist/allowlist table:

```
(host)[node] (config) #whitelist-db rap-local-switch-list del mac-address
00:16:CF:AF:3E:E1 / allowlist-db rap-local-switch-list del mac-address
00:16:CF:AF:3E:E1
```

Related Command

Command	Description
whitelist-db rap add /allowlist-db rap add	Add an entry into the remote AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whitelist-db rap-master-switch-list/allowlist-db rap-master-switch-list

```
whitelist-db rap-master-switch-list /allowlist-db rap-master-switch-list
  del mac-addr <mac-address>
  purge
```

Description

This command deletes a Mobility Conductor from the master/conductor switch table used by the Remote AP whitelist/allowlist.

Each managed device with Remote APs managed through a Remote AP whitelist/allowlist has a master/conductor switch whitelist/allowlist which contains the IP and MAC addresses of its Mobility Conductor. If your network has a redundant Mobility Conductor, then this list will contain more than one entry.



Though you can delete an entry from the master/conductor switch whitelist/allowlist, you should do so only if you have removed a master/conductor switch from the network. Deleting a valid Mobility Conductor from the master/conductor switch whitelist/allowlist can cause errors in your network.

Parameter	Description
<code>del mac-address <mac-address></code>	Remove a single Mobility Conductor from the master/conductor whitelist/allowlist.
<code>purge</code>	Clear all Mobility Conductors from the Registered master/conductor switch table.

Example

The following example removes a Mobility Conductor from the master/conductor switch whitelist/allowlist table:

```
(host) [node] (config) #whitelist-db rap-master-switch-list del mac-address
00:16:CF:AF:3E:E1 / allowlist-db rap-master-switch-list del mac-address
00:16:CF:AF:3E:E1
```

Related Command

Command	Description
whitelist-db rap add /allowlist-db rap add	Add an entry into the remote AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

allowed-address-list

```
allowed-address-list  
  ipv4  
  ipv6
```

Description

This command configures addresses exempted when the deny-inter-user-bridging is enabled.

Parameter	Description
ipv4	This parameter specifies the IPv4 address to be added to the allowed address list.
ipv6	This parameter specifies the IPv6 address to be added to the allowed address list.

Example

```
(host) [mynode] #allowed-address-table ipv4 10.12.133.14  
(host) [mynode] #allowed-address-table ipv4 10.12.133.15
```

Related Commands

Command	Description
no allowed-address-list	This command is used to remove the IP addresses that were added using allowed-address-list command.
show allowed-address-list	This command displays the list of allowed addresses that are exempted.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and managed device.

allow-sso

```
allow-sso <username> <role>
```

Description

This command configures the AMP SSO for a user name.

Parameter	Description
username	Enter the user name.
role	Enter the role of the user.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

am

```
scan ip-addr <ipaddr> <channel> [band | bssid <bssid>]
test ip-addr <ip-addr>
  auto-device-creation
    start interval <interval> phy-type {80211a|80211g}
    stop
  create-device
    ap phy-type {80211a|80211g} [bssid <bssid>] [mac <mac_address>]
    client phy-type {80211a|80211g} [bssid <bssid>] [mac <mac_address>]
  ev-gen event_id <event_id> trap_id <trap_id> [ADDITIONAL_INFO <ADDITIONAL_
INFO> | ADDRESS_TYPE <ADDRESS_TYPE> |
  AP_CHANNEL <AP_CHANNEL> | AP_LOCATION <AP_LOCATION> |
  AP_MAC_ADDRESS <AP_MAC_ADDRESS> | AP_RADIO_NUM <AP_RADIO_NUM> |
  ASSOCIATION_TYPE <ASSOCIATION_TYPE> | CONF_LEVEL <CONF_LEVEL> |
  FRAME_TYPE <FRAME_TYPE> | INTERFERING_AP_INFO_URL <INTERFERING_AP_INFO_URL>
  | MATCHED_IP <MATCHED_IP> | MATCHED_MAC <MATCHED_MAC> |
  NODE_MAC <NODE_MAC> | RECEIVER_MAC <RECEIVER_MAC> | ROGUE_INFO_URL <ROGUE_
INFO_URL> | SIGNATURE_NAME <SIGNATURE_NAME> | SNR <SNR>
  SOURCE_MAC <SOURCE_MAC> | SPOOFED_FRAME_TYPE <SPOOFED_FRAME_TYPE> | TARGET_
AP_BSSID <TARGET_AP_BSSID> | TARGET_AP_SSID <TARGET_AP_SSID> | TRANSMITTER_
MAC <TRANSMITTER_MAC>]
  fake-noise
  rap-ack-responses
  rssi
  suspect-rap bssid <bssid> match-type <match-type> match-method <match-method>
  wired-mac
    add {bssid <bssid> mac <mac>|enet-mac <enet-mac> mac <mac>|prop-wm mac <mac-
addr>|system-gw-wm mac <mac>|system-wm mac <mac>}
    remove {bssid <bssid> mac <mac>|enet-mac <enet-mac> mac <mac>|prop-wm mac
<mac>|system-gw-wm mac <mac>|system-wm mac <mac>}
  zero-wait-dfs
```

Description

The `scan` sub-command enables channel scanning for the specified air monitor. In addition, the `test` sub-command enables the client to test an air monitor. These commands are intended to be used with an AP that is configured as an air monitor.

Parameter	Description
<code>scan</code>	Enable or disable channel scan.
<code>ip-addr <ip-addr></code>	IP address of the air monitor to be scanned.
<code><channel></code>	Channel to which the scanning is tuned. Set to 0 to enable scanning of all channels.
<code>band</code>	Specify the band value from one of the following: <ul style="list-style-type: none">2.4 GHz

Parameter	Description
	<ul style="list-style-type: none"> 5 GHz 6 GHz
<code>bssid <bssid></code>	BSSID of the air monitor.
<code>test</code>	Enables the client to test an air monitor.
<code>ip-addr <ip-addr></code>	IP address of the air monitor.
<code>auto-device-creation</code>	<p>Sets the AP mode to add a monitored device and client at every interval.</p> <ul style="list-style-type: none"> start stop <p>Intervals are written as time in seconds.</p>
<code>interval <interval></code>	Sets the interval in seconds at which the new AP and client devices are added.
<code>phy-type {80211a 80211g}</code>	<p>Sets the band of the device.</p> <ul style="list-style-type: none"> 80211a for <i>a</i> band 80211g for <i>g</i> band
<code>create-device {ap client}</code>	<p>Creates an AP or client device.</p> <ul style="list-style-type: none"> ap client
<code>phy-type {80211a 80211g}</code>	<p>Specifies the band for the device.</p> <ul style="list-style-type: none"> 80211a 80211g
<code>bssid <bssid></code>	Specifies the bssid of the new device
<code>mac <mac></code>	Specifies the wired-mac address of the new device
<code>ev-gen</code>	Create an IDS event from the AP.
<code>event_id <event-id></code>	Specifies the event id to generate for the event.
<code>trap_id <trap_id></code>	<p>Specifies the trap id to generate or use 65535 if there are no traps. The various trap IDs are explained here:</p> <ul style="list-style-type: none"> ADDITIONAL_INFO—Additional information for syslog ADDRESS_TYPE—Address type (an integer because it is enum) AP_CHANNEL—Detecting AP channel or target channel AP_LOCATION—Detecting AP Name

Parameter	Description
	<ul style="list-style-type: none"> ▪ AP_MAC_ADDRESS—Detecting AP MAC ▪ AP_RADIO_NUM—Detecting AP Radio ▪ ASSOCIATION_TYPE—Association Type ex. Association To Rogue ▪ CONF_LEVEL—Confidence level of suspected rogue (5-100) ▪ FRAME_TYPE—Frame type (an integer because it is enum) ▪ INTERFERING_AP_INFO_URL—URL ▪ MATCHED_IP—Matched IP for classification ▪ MATCHED_MAC—Matched MAC for classification ▪ NODE_MAC—Node MAC ▪ RECEIVER_MAC—Receiver MAC ▪ ROGUE_INFO_URL—URL ▪ SIGNATURE_NAME—Name of signature matched ▪ SNR—Signal-to-Noise Ratio ▪ SOURCE_MAC—Source MAC ▪ SPOOFED_FRAME_TYPE—Spoofed Frame type (EAP Success) ▪ TARGET_AP_BSSID—Target AP BSSID ▪ TARGET_AP_SSID—Target AP SSID ▪ TRANSMITTER_MAC—Transmitter MAC
fake-noise	Generate fake noise floor value.
rap-ack-responses	Enable or disable rap ack responses for an AP.
rssi	Test RSSI.
suspect-rap	Test the suspect remote AP feature.
bssid <bssid>	Specifies the BSSID of monitored AP.
match-type <match-type>	Specifies the match type.
match-method <match-method>	Specifies the match method.
wired-mac {add remove}	Tests the rogue AP classification feature. Specifies the wired MAC table.
bssid <BSSID> mac <mac>	Specifies BSSID of monitored AP and wired-MAC address.
enet-mac <enet-mac> mac <mac>	MAC address of ENET interface of AP and wired-MAC address.

Parameter	Description
<code>prop-wm mac <mac></code>	Specifies the propagate wired-MAC
<code>system-gw-wm mac <mac></code>	Specifies the system gateway MAC.
<code>system-wm mac <mac></code>	Specifies the system wired-MAC.
<code>zero-wait-dfs</code>	Start or stop zero wait DFS testing for an AP.

Example

The following command sets the air monitor to scan all channels:

```
(host) (config) #am scan 10.1.1.244 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

amon cert

```
amon cert <cert-name>
```

Description

This command specifies the certificate name for Amon secure.

Parameter	Description
<code><cert-name></code>	Specify the certificate name.

Example

The example below enables AMON UDP.

```
(host) [mynode] (config) #amon cert
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

amon msg-buffer-size

amon msg-buffer-size <msg-buffer-size>

Description

This command modifies the size of AMON packets on the managed device.

Parameter	Description
<msg-buffer-size>	The size of AMON packets on the managed device. 1152-40000 1264

Example

The following command caps the AMON message size at 1500 bytes:

```
(host) [mynode] (config) #amon msg-buffer-size 1500
```

Related Commands

Release	Modification
show amon msg-buffer-size	Displays the size of AMON packets on the managed device.

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>msg-buffer-size</code> range was modified.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

amon source-interface

```
amon source-interface <vlan-num>
```

Description

This command specifies the IPv4 address of the VLAN as the source IP address.

Parameter	Description
<vlan-num>	The IPv4 address of the VLAN.

Example

The following example sets the VLAN number.

```
(host) [mynode] (config) #amon source-interface <vlan-num>
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

amon udp

[no] amon udp

Description

Enable the AirWave server to allow traffic on UDP port 8211.

Issue the `no amon udp` command to disable AMON UDP and re-enable it again using the command `amon udp`.

Example

The example below enables AMON UDP.

```
(host) [mynode] (config) #amon udp
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap am-filter-profile

```
ap am-filter-profile {default | <profile-name>}
  allow-ap-group
  allow-self
  ap-group <ap-group>
  ap-name <ap-name>
  clone
  filter-enable
  no
```

Description

This command configures an AM filter.

Parameter	Description
am-filter-profile <profile-name>	Name of this instance of the profile
allow-ap-group	Allows all APs in the same group as the AP
allow-self	Allows AP to hear its own frames
ap-group <ap-group>	Allows all APs in the group
ap-name <ap-name>	Name of AP to allow
clone {default <source>}	Copy data from another AM filter
filter-enable	Enable AM filtering
no	Delete command

Example

The following command allows AM filtering for all APs in the test1 group:

```
(host) [mynode] (config) #ap am-filter-profile test
(host) [mynode] (AM Filter "test") #ap-group test1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap ap-blacklist-time / ap ap-denylist-time

```
ap ap-blacklist-time <ap-blacklist-time>/ap ap-denylist-time <ap-denylist-time>
no...
```

Description

This command determines the time, in seconds, for which a client is manually blocked.

Parameter	Description
<ap-blacklist-time>/<ap-denylist-time>	The time, in seconds, that the client remains blocked.
no ap ap-blacklist-time	Removes the blacklist time configured using the <code>ap-blacklist-time</code> command and restores the default value of 3600 seconds.

Example

The following is an example of the `ap ap-blacklist-time/ap ap-denylist-time` command:

```
(host) [mynode] (config) #ap ap-blacklist-time 55/ap ap-denylist-time 55
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.7.1.1	The <code>no ap ap-blacklist-time</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on the Mobility Conductor.

ap arm client-match

```
ap arm client-match
  activate rules file-name <file-name>
  restore rules
```

Description

This command allows the managed device to use a newer set of ClientMatch rules without updating the entire operating system, reducing network downtime.

The ClientMatch rules that manage client associations are primarily based upon the client RF environment, and apply uniformly to all types of clients, regardless of device type or operating system. ArubaOS supports incremental updates to ClientMatch rules to support network devices running newer operating systems that may be incompatible with the existing ClientMatch client association rules. This feature allows the managed device to use a newer set of ClientMatch rules without updating the entire operating system, reducing network downtime.

Parameter	Description
<code>activate rules file-name <file-name></code>	File name of the client-match rules update package.
<code>restore rules</code>	Issue this command to remove an imported client-match rules update package and restore the default ClientMatch values.

Example

Use the WebUI or CLI to upload a custom update file of client -match rules to the /flash/config folder on Mobility Conductor. This feature is not available for stand-alone controller deployments.

```
(host)[mm](config)# copy tftp: <tftphost> <filename> flash: <destname>
(host)[mm](config)# copy ftp: <ftphost> <user> <password> flash: <destname>
(host)[mm](config)# copy scp: <scphost> <username> <password> flash:
<destname>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Mobility Conductor	Base operating system.	Config mode on Mobility Conductor.

ap authorization-profile

```
ap authorization-profile {default | <profile-name>}
  ap-authorization-group <profile-name>
  clone {default | <source>}
  no
```

Description

The AP authorization-profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows a user to connect to an unauthorized remote AP through a wired port and then enter a corporate username and password. Once a valid user has authorized the remote AP, the AP will be permanently marked as authorized on the network and will then download the configuration assigned to that AP by its permanent AP group.

Parameter	Description
ap authorization-profile <profile-name>	Name of this instance of the profile. 1-63 default
ap-authorization-group <profile-name>	Name of a configuration profile to be assigned to the group unauthorized remote APs.
clone {default <source>}	Copy data from another authorization profile. default
no	Delete command.

Example

The following command creates a new authorization profile with a non-default configuration for unauthorized remote APs:

```
(host) [mynode] (config) #ap authorization-profile default2
(host) [mynode] ((AP Authorization profile "default2") #authorization-group
NoAuthApGroup2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap ble-configure

```
ap ble-configure
  {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
  cfg-ble-mac <cfg-ble-mac-addr>
  delete-slot slot <slot>
    interval <interval>
  generic-payload <generic-payload> slot <slot>
    interval <interval>
  major <major>
    minor <minor>
      UUID <uuid> interval
```

Description

This command configures beacon attributes like major, minor, and uuid on a managed device.

Syntax

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
cfg-ble-mac <cfg-ble-mac-addr>	The MAC address of the BLE device to be configured.
delete-slot slot <slot>	Delete beacon config of the specified slot number. For creating or deleting the beacon config, available range is [0,2]. For deleting beacons from all slots, 3 is reserved.
generic-payload <generic payload>	Custom Beacon payload. This is a variable length hex string.
major <major>	The IBeacon major number. 0-65535
minor <minor>	The IBeacon minor number. 0-65535
uuid <uuid>	The UUID of IBeacon. The UUID is always a fixed length hex string, for example: 4152554E-F99B-4A3B-86D0-947070693A78
interval	Beaconing interval in millisecond. 0-65535

Example

The following command sets beacon attributes:

```
[mynode] #ap ble-configure ap-name 325_2 cfg-ble-mac 84:eb:18:18:5e:f8 major  
1000 minor 2000
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap ble-init-action

ap ble-init-action ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ipv6 address>

Description

This command initiates BLE action for APs.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ipv6 address>	IPv6 address of the AP.
add-log-level-str	This parameter will define BLE daemon log level as one of the following value: <ul style="list-style-type: none">ageoutamonapbat-https- jsonat-websocket-protobufAzure -IoT Hubbcnerrbcntl vbeaconbmreqcfgupdatecfgupdateerrdevmgmtenocanerrorfw-upgradefw-upgradeerrinfoiot-gwtagswarningzf
ap-sleep-duration-min	This parameter specifies AP sleep duration in minutes.
apb-clear-msg	This parameter clears incoming message buffer.
apb-power-reset	This parameter provides power-on reset for the on-board BLE radio.

Parameter	Description
apb-switch-bl	This parameter switches APB to bootloader image during image upgrades.
azure-clear-flash-provisioning	This parameter clears DPS provisioning information in the AP.
azure-dps-provisioning	This parameter forces AP to execute DPS provisioning.
azure-iothub-connect	This parameter forces AP to execute IoT Hub connecting.
clear-all-beacons	This parameter deletes all beacon data.
clear-all-log-mac-filters	This parameter clears all the BLE daemon log MAC filters.
clear-log-mac-filter	This parameter clears the BLE daemon log MAC filter.
input-filter-disable	This parameter disables input filter for storing devices in the BLE table.
input-filter-enable	This parameter enables input filter for storing devices in the BLE table.
iot-coex-disable	This parameter disables IoT coexistence for onboard IoT radio.
iot-coex-enable	This parameter enables IoT coexistence for onboard IoT radio.
log-level	BLE daemon log level specified as a number.
log-level-str	BLE daemon log levels specified as comma-separated values (without quotes). Possible values: 'info','warning','error','ageout','bmreq','fw-upgrade','fw-upgradeerr','cfgupdate','cfgupdateerr','beacon','bcntlv','bcnerr','apb','tags','zf','amon','iot_gw','at-https-json','at-websocket-protobuf'.
log-mac-filter	BLE daemon log MAC filter.
msg-select	Set bits to enable specific messages from APB to controller BLE Daemon - refer to BLE config CLI cmd.
ota-fw-upgrade	Over the Air firmware upgrade for onboard BLE.
remove-beacon-mac	Delete beacon with matching MAC address.
send-apb-update	Send APB info update to BLE Relay on controller.
send-update	Send IoT payload message to BMC immediately.
start-log	Enable BLE Daemon logging.

Parameter	Description
stop-log	Disable BLE Daemon logging.
zigbee permit-joining restart	Re-start zigbee initial permit joining duration.
all	Re-start all devices.
mac <mac-address>	Re-start specific devices.

Command History

Release	Modification
ArubaOS 8.7.0.0	The fololowing parameters are introduced: <ul style="list-style-type: none"> ■ input-filter-disable ■ input-filter-enable
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

apboot

```
apboot {all [global|local]|ap-group <ap-group> |ap-name <ap-name>|ip-addr <ipaddr>|ip6-addr <ip6addr>|wired-mac <macaddr>}
```

Description

This command reboots the specified APs.

You should not normally need to use this command as APs automatically reboot when you reprovision them. Use this command only when directed to do so by your Aruba representative.

Parameter	Description
all	Reboot all APs.
global	Reboot APs on all controllers.
local	Reboot only APs registered on this controller. This is the default.
ap-group	Reboot APs in a specified group.
ap-name	Reboot the AP with the specified name.
ip-addr	Reboot the AP at the specified IP address.
ip6-addr	Reboot the AP at the specified IPv6 address.
wired-mac	Reboot the AP at the specified MAC address.

Example

The following command reboots a specific AP:

```
(host) [mynode] (config)# apboot ap-name Building3-Lobby
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

ap clarity-synthetic

```
ap clarity-synthetic {ap-name <ap-name> | wired-mac <wired-mac>}
  amsip-addr <amsip-addr> forward-mode
    gre test-id <test-id> | web-sockets test-id <test-id>
    mixed-mode band <a|g> | station-mode
  reset
```

Description

This command allows configuration of the Clarity-Synthetic feature. Clarity Synthetic enables the controller to select and convert a supported AP to client mode. The converted AP acts like a Wi-Fi client and starts synthetic data transaction within the network to monitor and detect the network health.

The Clarity Synthetic feature is supported on 200 Series, 210 Series, and 220 Series access points. This feature helps in detecting network health by using synthetic transaction from a Wi-Fi client. This feature converts the radios of a supported AP to change from AP mode to station mode.

Parameter	Description
<code>ap clarity-synthetic</code> {ap-name <ap-name> wired-mac <wired-mac>}	Specifies the name of the AP or the AP wired MAC address.
<code>amsip-addr <amsip-addr> forward-mode</code>	IP address of Clarity synthetic Server with the forward mode specified for test
<code>gre test-id <test-id> </code> <code>web-sockets test-id <test-id></code>	GRE mode of forwarding or the web sockets mode of forwarding with unique test id string
<code>mixed-mode band <a g> station-mode</code>	Specifies if AP operates in mixed mode (for either the a or g band) or in only station mode
<code>reset</code>	Resets the AP from Clarity Synthetic mode.

Example

The following command configures the IP address of the Clarity-Synthetic server (in the forward mode used for test) and specifies the GRE mode of forwarding for an AP working in the *a* band :

```
(host) [mynode] #ap clarity-synthetic wired-mac ac:a3:1e:d6:30:f0 amsip-addr
5.6.7.5 forward-mode gre test-id 5 mixed-mode band a
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Mobility Conductor	Base operating system.	Enable or Config mode on Mobility Conductor.

apconnect

```
apconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command instructs a mesh point to disconnect from its current parent and connect to a new parent.

To maintain a mesh topology created using the **apconnect** command, Aruba suggests setting the mesh reselection-mode to **reselect-never**, otherwise the normal mesh reselection mechanisms could break up the selected topology.

Parameter	Description
ap-name <name>	Specify the name of the mesh point to be connected to a new parent.
bssid <bssid>	Specify the BSSID of the mesh point to be connected to a new parent.
ip-addr <ipaddr>	Specify the IP address of the mesh point to be connected to a new parent.

Example

The following command connects the mesh point “meshpoint1” to a new parent with the specified BSSID.

```
(host) [mynode] (config) #apconnect ap-name meshpoint1 parent-bssid  
00:12:6d:03:1c:f1
```

Related Commands

Command	Description
ap mesh-radio-profilereselection-modereselect-never	Use this command to prevent the AP from re-selecting a new parent.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

ap consolidated-provision info

ap consolidated-provision info

Description

This command will get all the APs consolidated provision details and store in ap_provision_info.txt.

Example

```
(host) [mynode] ap consolidated-provision info  
Command Completed Successfully, Please retrieve results in ap_provision_  
info.txt file
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

ap convert

```
ap convert
  active {all-aps|specified-aps}
  add {ap-group|ap-name}
  cancel
  clear-all
  delete {ap-group|ap-name}
  pre-validate {all-aps|specified-aps}
```

Description

This command is used to convert a Campus AP or a Remote AP to an Instant AP that is managed by Aruba Central. However, Aruba does not support this feature for Instant AP deployments that are managed through AirWave or local WebUI, and recommends using this command only in lab or test environments for such deployments.



- This feature is not supported on 320 Series AP models with 256 MB of SDRAM, manufactured between August 2015 and January 2016. These 320 Series AP models have a serial number that begins with DD (for example, DD0003824).
- The converted APs are limited to the highest supported version of the corresponding Instant APs. For example, if IAP-225 runs only up to Aruba Instant 8.6.0.0 version, the converted AP-225 will also support up to Aruba Instant 8.6.0.0 version.

Parameter	Description
<code>active {all-aps specified-aps}</code>	Convert active Campus AP or Remote AP to Instant APs that are managed by Aruba Central. NOTE: You can activate Instant AP conversion for all registered APs or APs specified by <code>ap convert ap-group</code> and/or <code>ap convert ap-name</code> commands.
<code>add {ap-group ap-name}</code>	Add AP group or AP name to list for AP conversion.
<code>cancel</code>	Cancel conversion. Any APs that are currently downloading the new image will continue to do so.
<code>clear-all</code>	Remove all AP groups and AP names from list for conversion.
<code>delete {ap-group ap-name}</code>	Delete AP group or AP name from list for conversion.

Parameter	Description
pre-validate {all-aps specified-aps}	Pre-validate the Campus AP or Remote AP to Aruba Activate or Central connection. NOTE: You can validate all registered APs or APs specified by <code>ap convert ap-group</code> and/or <code>ap convert ap-name</code> commands.

Example

The following example displays the options to convert all active Campus APs:

```
(host) [mynode] #ap convert active all-aps
activate           Convert CAP from activate.
local-flash       Convert CAP from MD local flash.
server            Convert CAP from local server.
```

The following example displays the options to convert specific Campus AP or Remote APs from local servers:



Before issuing the command, ensure that the **Read** permission is included for **Others** for the AP image files on the SCP server. This makes sure that the AP image file can be read during the conversion process.

```
(host) [mynode] #ap convert active specific-aps server
ftp               Download image from ftp server.
http              Download image from http server.
https             Download image from https server.
scp               Download image from scp server.
tftp              Download image from tftp server.
```

The following example validates Campus APs or Remote APs to Activate or Central connection:

```
(host) [mynode] (config) #ap convert pre-validate all-aps
WARNING: This command will validate AP to Activate/Central connection, which
include NTP time sync. Do you want to proceed with the operation? [y/n]: y
(host) [mynode] (config) #
```

Command History

Release	Description
ArubaOS 8.7.0.0	The <code>pre-validate</code> parameter was introduced.

Release	Description
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

ap-crash-transfer

ap-crash-transfer

Description

This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

The command `ap system-profile <profile> dump-server <server>` specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the `ap-crash-transfer` command to save dump files to the controller flash memory.

If you define a dump server and issue the `ap-crash-server` command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)[mynode] (config) #ap-crash-transfer
```

Related Commands

Command	Description
show ap-crash-transfer	This command shows if AP coredump files can be transferred to controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap debug dot 11r remove-key

```
ap debug dot 11r remove-key <mac>  
[ap-name <ap-name> | ip-addr <ip-addr>| ip6-addr <ip6-addr>]
```

Description

Use this command to remove an r1 key from an AP when the AP does not have a cached r1 key during Fast BSS Transition roaming.

Parameter	Description
<mac>	MAC address of the client.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.

Examples

You can use the following command to remove an r1 key from an AP when the AP does not have a cached r1 key during Fast BSS Transition roaming.

```
(host) [mynode] #ap debug dot11r remove-key <mac> ap-name <ap-name> | ip-  
addr <ip-addr>  
(host) [mynode] #ap debug dot11r remove-key 00:50:43:21:01:b8 ap-name  
MAcage-105-GL
```

Execute the following command to check if the r1 key is removed from the AP:

```
(host) [mynode] #show ap debug dot11r state ap-name MAcage-105-GL  
Stored R1 Keys  
-----  
Station MAC  Mobility Domain ID  Validity Duration  R1 Key  
-----
```

Related Commands

Command	Description
show ap debug dot11r efficiency	Use this command to check if the r1 key is removed from an AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap debug advanced-stats

```
ap debug advanced-stats {ap-name <ap-name>}|{ ip-addr <ip-addr>}|{ ip6-addr <ip-addr>}
```

Description

Issue this command under the supervision of Aruba technical support to enable the collection and display of advanced AP debugging information.

The additional information collected when advanced net80211 or radio statistics are enabled on an AP appears in the output of the [show ap debug radio-stats](#) command.

Parameter	Description
ap-name <ap-name>	Name of the AP for which you want to record advanced debugging information.
ip-addr <ip-addr>	IP address of the AP for which you want to record advanced debugging information.
ip6-addr <ip6-addr>	IPv6 address of the AP for which you want to record advanced debugging information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap debug client-trace stop

```
ap debug client-trace stop  
  {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}<mac>
```

Description

This command stops tracing management packets from a client MAC address. You must issue the command only under the guidance of Aruba technical support. This command is supported on 100 Series, 120 Series, and 130 Series access points only.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IPv4 address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<mac>	MAC address of the client.

Related Commands

Command	Description
ap debug client-trace start	Use this command to trace management packets from a client MAC address.
show ap debug client-trace	Use this command to show counts of different types of management data frames traced from a client MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Conductor.

ap debug client-trace start

```
ap debug client-trace start
  {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}<mac>[length-range
  {max|min<min>}]
```

Description

This command traces management packets from a client MAC address. You must issue the command only under the guidance of Aruba technical support. This command is supported on 100 Series, 120 Series, and 130 Series access points only.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IPv4 address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<mac>	MAC address of the client.
length-range {max min<min>}	The maximum and minimum length range of data packet. 1-65535 bytes

Related Commands

Command	Description
ap debug client-trace stop	Use this command to stop tracing management packets from a client MAC address.
show ap debug client-trace	Use this command to show counts of different types of management data frames traced from a client MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable mode on Mobility Conductor.

ap debug openflow

```
ap debug openflow flows  
  delete-all {ap-name <ap-name> |ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command deletes all the OpenFlow flows, and should only be used under the guidance of Aruba technical support.

Parameter	Description
flows	A list of OpenFlow flows.
delete-all	Deletes all OpenFlow flows. <ul style="list-style-type: none">■ ap-name - name of the AP to be deleted.■ ip-addr - IPv4 address of the AP.■ ip6-addr - IPv6 address of the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Conductor.

ap debug radio-diag-log

```
ap debug radio-diag-log {start | stop} {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} grep <pattern> [size <num-bytes>]
```

Description

This command collects WLAN firmware diagnostic logs to facilitate firmware debugging. Configure the **dump-collection-profile** to use this command. When the **radio-diag-log** collection is stopped using `ap debug radio-diag-log stop` command, the log file is automatically transferred to the dump server that is configured in **dump-collection-profile**.

Parameter	Description
start	Starts logging the radio diagnostic messages.
grep	Stores only the filtered output. The pattern supports the same options as the AP shell's grep. NOTE: The grep pattern is mandatory.
stop	Stops logging the radio diagnostic messages.
size	Size of the radio diagnostic messages.

Example

The following command collects the grep output:

```
(host) [mynode] #ap debug radio-diag-log start ap-name <name> grep "-e WMI -e WAL"
```

Related Commands

Command	Description
show ap debug radio-diag-log status	This command displays the current diagnostic logging status of an AP.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
AP-534, AP-535, AP-555 access points	Base operating system.	Enable mode on Mobility Conductor.

ap debug radio-event-log

```
ap debug radio-event log [start|stop] [ap-name <name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>] radio <0|1> events [all|ani|hex|rcfind|rcupdate|rx|size|text|tx]>
```

Description

Start and stops packet log capture of radio events for debugging purposes, and sends a log file of the events to a dump server when logging stops.

Parameter	Description
start	Start Wi-Fi packet log capture.
ap-name <ap-name>	Name of the AP for which you want to capture packet log events.
radio 0 1	Include this parameter to start or stop packet log capture for the specified radio.
events	Classification the event type to capture, can be hex and multiple, default all. <ul style="list-style-type: none">■ all: Capture all of the following types of radio events■ ani : Adaptive Noise Immunity control events■ hex: Hex format of event tx=0x1 rx=0x2 rcfind=0x4 rcupdate=0x8 ani=0x10 text=0x20■ rcfind: Transmission (Tx) control event■ rcupdate: Transmission (Tx) rate update event■ rx: Received (Rx) status register event■ size: radio log size,range 1024-10485760 bytes(1KB-10MB), Default:3145728 bytes(3MB)■ text: Text record event■ tx: Transmission (Tx) control and Tx status register event
ip-addr <ip-addr>	IPv4 address of the AP for which you want to capture packet log events.
ip6-addr <ip6-addr>	IPv6 address of the for which you want to capture packet log events.
stop	Stop Wi-Fi packet log capture and send a log file of the events to a dump server.

Example

The following commands starts and stops a Wi-Fi radio event log:

```
(host) [mynode] #ap debug radio-event-log start ap-name 6c:f3:7f:c6:71:90  
radio 0 events all
```

```
(host) [mynode] #ap debug radio-event-log stop ap-name 6c:f3:7f:c6:71:90
radio 0
```

Related Commands

Command	Description
show ap debug dot11r efficiency	Use this command to display the Radio log capture status.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap debug radio-registers dump

```
ap debug radio-registers dump [[filename <filename> {all|interrupt|qcu |radio}]ap-name <name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
```

Description

This command collects specified radio-register information for debugging purposes, dumps the registers into a local file, and will automatically transfer the file to the dump-server that is configured in ap-system-profile.

Parameter	Description
ap-name	Name of the access point.
filename	Name of file where information is collected.
all	All registers interrupted.
interrupt	Interrupt related registers.
qcu	Collect QCU information.
radio	Radio ID (0 or 1).
ip-addr	Collect radio register information for this specific AP radio.
ip6-addr	Collect radio register information for the AP assigned to this ipv6 address.

Example

The following command collects all radio registers from **myap1** into a file called **myradioregfile**:

```
(host) [mynode] #ap debug radio-registers dump ap-name myap1 filename myradioregfile all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
802.11n-capable APs	Base operating system.	Enable mode on Mobility Conductor.

ap debug stm-trace

```
ap debug stm-trace category  
[ip-addr <ip-addr> | loglevel | mac <mac>]
```

Description

This command enables / disables stm-trace categories.

Parameter	Description
category	The trace category to be enabled or disabled. <ul style="list-style-type: none">■ all - Traces all categories■ amon - Traces in the category of AMON■ auth - Traces in the category of authentication■ bss - Traces in the category of BSSIDs■ cluster - Traces in the category of cluster■ config - Traces in the category of configuration■ enet - Traces in the category of AP Enet port management■ gsm - Traces in the category of GSM■ radio - Traces in the category of radio■ sapm - Traces in the category of cluster■ sos - Traces in the category of SOS■ station - Traces in the category of stations■ syslog - Traces in the category of syslog■ system - Traces in the category of general system
ip-addr <ip-addr>	Trace events related to the AP IP address.
loglevel	The loglevel of the syslogs to be included in the trace. <ul style="list-style-type: none">■ alert - Trace all logs equal or higher than LOG_ALERT■ critical - Trace all logs equal or higher than LOG_CRIT■ debug - Trace all logs equal or higher than LOG_DEBUG■ emergency - Trace all logs equal or higher than LOG_EMERG■ error - Trace all logs equal or higher than LOG_ERR■ info - Trace all logs equal or higher than LOG_INFO■ notice - Trace all logs equal or higher than LOG_NOTICE■ warn - Trace all logs equal or higher than LOG_WARN
mac <mac>	Trace events related to the client MAC address.

Examples

You can use the following command to trace all events related to the IP address.

```
(host) [mynode] #ap debug stm-trace category all ip-addr <ip-addr>
```

```
(host) [mynode] #ap debug stm-trace category all 10.20.10.20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap deep-sleep

```
ap deep-sleep
ap-name <ap-name>
ip-addr <ip-addr>
ip6-addr <ip6-addr>
mac-list <mac_list>
wired-mac <wired_mac>
```

Description

This command is used to move the APs into deep-sleep mode.

Parameter	Description
ap-name	Name of an AP.
ip-addr	IP address of AP.
ip6-addr	IPv6 address of AP.
mac-list	Semicolon separated MAC address list. The maximum characters supported is 250.
wired-mac	The MAC address of an AP.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

apdisconnect

```
apdisconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command disconnects a mesh point from its parent.

Each mesh point learns about the mesh portal from its parent (a mesh node that is part of the path to the mesh portal). This command directs a mesh point to disassociate from its parent. The mesh point will attempt to associate with another neighboring mesh node, if available. The old parent is not eligible for re-association for 60 seconds after disconnection.

Syntax

Parameter	Description
ap-name	Specifies the name of the parent AP.
bssid	Specifies the BSSID of the parent AP.
ip-addr	Specifies the IP address of the parent AP.

Example

The following command disconnects a specific mesh point from its parent:

```
(host) [mynode] (config) #apdisconnect ap-name meshpoint1
```

Related Commands

Command	Description
apconnect	This command connects a mesh point to a new specified parent.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

ap deploy-profile

```
ap deploy-profile
  blacklist/denylist
  default-ap-group
  enable
  ip-range <start> <end>
  ipv6-range <start> <end>
  no
```

Description

This command applies the AP deployment policy to the default AP group, and/or to the list of AP MAC addresses included in the UAP blacklist/denylist table, and/or to the specified IP address range. The AP deployment policy redirects the applicable APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.

Parameter	Description
blacklist/denylist	Enables the blacklist/denylist policy. Applies the AP deployment policy to the APs whose MAC addresses are included in the UAP blacklist/denylist table.
default-ap-group	Applies the AP deployment policy to the default AP group.
enable	Enables the AP deploy profile. The policies configured are enforced only if this is enabled.
ip-range	Applies the AP deployment policy to the specified IPv4 address range. You can define up to 128 IPv4 address ranges.
<start>	Starting IPv4 address of the range.
<end>	Ending IPv4 address of the range.
ipv6-range	Applies the AP deployment policy to the specified IPv6 address range. You can define up to 128 IPv6 address ranges.
<start>	Starting IPv6 address of the range.
<end>	Ending IPv6 address of the range.
no	Removes the AP deploy profile configuration.

Example

The following set of commands enable the AP deployment policy :

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #enable
```

The following command applies the AP deployment policy to an IPv4 address range with a starting IP address of 1.1.1.1 and ending IP address of 1.1.1.10:

```
(host) [mynode] (ap deploy-profile) #ip-range <1.1.1.1> <1.1.1.10>
```

The following command enables the blacklist/denylist policy in the AP deploy profile:

```
(host) [mynode] (ap deploy-profile) #blacklist/denylist
```

The following command removes the AP deployment policy configuration:

```
(host) [mynode] (config) #no ap deploy-profile
```

Related Commands

Command	Description
show ap deploy-profile	The <code>show ap deploy-profile</code> command displays the complete list of IP address ranges to which the AP deployment policy is applied.
uap-blacklist / uap-denylist	This command adds AP MAC addresses to the UAP blacklist/denylist database. When the blacklist/denylist policy is enabled in the AP deploy profile, it is applied to this blacklist/denylist database entries.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap enet-link-profile

```
ap enet-link-profile {default | <profile>}
  clone {default | <source>}
  dot3az
  dot3bz
  duplex {auto | full | half}
  no ...
  poe
  speed {10 | 100 | 1000 | 2500 | 5000 | auto}
```

Description

This command configures the duplex and speed of the Ethernet port on the AP. The configurable speed is dependent on the port type.

Parameter	Description
ap enet-link-profile <profile>	Name of this instance of the profile. The name must be 1-63 characters long.
clone <source>	Name of an existing Ethernet Link profile from which parameter values are copied.
dot3az	Enable support for the 803.az Energy Efficient Ethernet standard, which allows the APs to consume less power during periods of low data activity. If this feature is enabled for an AP group, any APs in the group that do not support 803.az will ignore this setting. disabled
dot3bz	Enable support for IEEE 802.3bz standard. Only 330 Series access points are compliant with this standard. enabled
duplex	The duplex mode of the Ethernet interface, either full, half, or auto-negotiated. full, half, auto auto
no	Negates any configured parameter.
poe	Enables PoE for APs that support PoE.
speed	The speed of the Ethernet interface, either 10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps), or auto-negotiated. 10, 100, 1000, 2500, 5000, auto auto

Example

The following command configures the Ethernet link profile for full-duplex and 100 Mbps:

```
(host) [mynode] (config) #ap enet-link-profile enet
(host) [mynode] (AP Ethernet Link profile "enet") #duplex full
(host) [mynode] (AP Ethernet Link profile "enet") #speed 100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

apflash

```
apflash
  all {global|local}
  ap-group <ap-group>
  ap-name <ap-name>
  ap31x-ap32x backup partition
  ip-addr <ip-addr>
  wired-mac <wired-mac>
```

Description

This command re-flashes the specified AP. Execute this command under the guidance of Aruba technical support.

Parameter	Description
all	Re-flash all APs.
global	Re-flash all APs on all managed devices.
local	Re-flash all APs registered on this device. This is the default setting.
ap-group	Re-flash all APs in this group.
ap-name	Re-flash AP with this name.
ap31x-ap32x backup partition	Upgrades the backup partition of Aruba 310 Series and 320 Series access points running ArubaOS 6.4.x or earlier versions to the ArubaOS version running on the Mobility Conductor.
ip-addr	Re-flash AP with this IP address.
wired-mac	Re-flash AP with this MAC address.

Example

The following command re-flashes an AP with an AP name *ap-corp-325*:

```
(host) [mynode] #apflash ap-name ap-corp-325
```

Command History

Release	Modification
ArubaOS 8.6.017, 8.7.1.9, 8.9.0.3	The ap31x-ap32x backup partition parameter was introduced.
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ap flush-r1-on-new-r0

```
ap flush-r1-on-new-r0
```

Description

Use this command to enable or disable flushing of R1 keys, when R0 is updated for d-tunnel or bridge mode.

Example

The following example enables flushing of R1 keys:

```
(host) [mynode] (config) #ap flush-r1-on-new-r0
```

The following command displays the status of flushing of R1 keys:

```
(host) [mynode] (config) #show flush-r1-on-new-r0  
Fast Roaming flush-r1-on-new-r0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode or Config mode on the Mobility Conductor or the managed device.

ap gap-db

```
ap gap-db
[reinit-
resync lms {lms-ip <lms-ip>}|{lms-ip6 <lms-ip6>} [{ap-name <ap-name>}|{wired-mac
<wired-mac>}]
```

Description

Resynchronize an AP status on a managed device and Mobility Conductor.

A managed device sends AP status messages about the APs terminating on that managed device to Mobility Conductor. In the event that an AP state appears to be different between Mobility Conductor and the managed device, this command will resynchronize the AP status information by allowing the managed device and Mobility Conductor to exchange a list of APs.

Parameter	Description
reinit-db	Re-initialize GAP DB.
resync	Trigger a re-sync.
lms	Specify the managed device to be synchronized.
lms-ip <lms-ip> lms-ip6 <lms-ip6>	Synchronize the status of all APs terminating on the specified Managed device. Specify either the IPv4 address or the IPv6 address of the managed device.
ap-name <ap-name>	Synchronize only the AP with the specified AP name.
wired-mac <wired-mac>	Synchronize only the AP with the specified MAC address.

Example

The following command triggers a resynchronization for an IPv4 address of the managed device.

```
(host)[mynode]#ap gap-db resync lms lms-ip 10.20.10.20
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap get-crash-dumps

```
ap get-crash-dumps
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command allows AP crash dump files to be transferred to the controller flash memory on demand from the AP flash memory.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.

Example

```
(host) [mynode] #ap get-crash-dumps ap-name ap535
```

Related Commands

Command	Description
show ap get-crash-dumps-status	This command displays the status of the crash dump file transfers to a controller.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
AP-534, AP-535, AP-555 access points	Base operating system.	Config mode on Mobility Conductor.

ap general-profile

```
ap general-profile
  keepalive-timeout
  no
  periodic-sync
  stale-ap-ageout-time
  sync-interval
```

Description

This command configures the general profile of an AP.

Parameter	Description
keepalive-timeout	Specify the timeout interval in minutes for AP keepalive. 15-10080
no	Negates any previous configuration.
periodic-sync	Enables AP State periodic sync.
stale-ap-ageout-time	Specify the time interval in hours after which AP information is cleared automatically. 0-240 By default, this value is 0 and the auto clear function is disabled.
sync-interval <sync-interval>	Specifies AP State sync interval in minutes. 5-1440

Example

The following example enables the AP state periodic sync of an AP:

```
(host) [mynode] (config) #ap general-profile
(host) [mynode] (ap general-profile) #periodic-sync
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap-group

```
ap-group {default | <profile-name>}
  am-filter-profile {default | <profile-name>}
  airslice-profile <name>
  airslice-visibility record-limit <record-count>
  ap-multizone-profile {default | <profile-name>}
  ap-system-profile {default | <profile-name>}
  authorization-profile {default | <profile-name>}
  clone {default | <source>}
  dot11-60GHz-radio-profile {default | <profile-name>}
  dot11-6GHz-radio-profile {default | <profile-name>}
  dot11a-radio-profile {default | <profile-name>}
  dot11a-secondary-radio-profile {default | <profile-name>}
  dot11a-traffic-mgmt-profile {default | <profile-name>}
  dot11g-radio-profile {default | <profile-name>}
  dot11g-traffic-mgmt-profile {default | <profile-name>}
  enet-usb-port-profile {default | noAuthWiredPort | shutdown | <profile-name>}
  enet0-port-profile {default | <profile-name>}
  enet1-port-profile {default | <profile-name>}
  enet2-port-profile {default | <profile-name>}
  enet3-port-profile {default | <profile-name>}
  enet4-port-profile {default | <profile-name>}
  event-thresholds-profile {default | <profile-name>}
  gps-service-profile <profile-name>
  ids-profile {default | <profile-name>}
  iot radio-profile <profile-name>
  mesh-accesslist-profile {default | <profile-name>}
  mesh-cluster-profile {default | <profile-name>} [priority <1-16>]
  mesh-radio-profile {default | <profile-name>}
  no ...
  provisioning profile {default | <profile-name>}
  regulatory-domain-profile {default | <profile-name>}
  rf-optimization-profile {default | <profile-name>}
  usb-profile {default | <profile-name>}
  virtual-ap {default | <profile-name>}
  wifi-uplink-profile <wifi-uplink-profile> {priority}
  zigbee service-profile <profile-name>
```

Description

This command configures an AP group. AP groups are at the top of the configuration hierarchy. An AP group collects virtual AP definitions and configuration profiles, which are applied to APs in the group.

Parameter	Description
ap-group <profile-name>	Profile name that identifies the AP group. The name must be 1–63 characters long.

Parameter	Description
	NOTE: You cannot use quotes (") in the AP group name.
am-filter-profile <profile-name>	Configures the AM filter profile.
airslice-profile <name>	Configures the Air Slice profile.
airslice-visibility record-limit <record-count>	Defines the maximum number of records stored for clients.
ap-multizone-profile <profile-name>	Configures the AP MultiZone profile.
ap-system-profile <profile-name>	Configures AP administrative operations, such as logging levels. See ap system-profile on page 354 .
authorization-profile <profile-name>	Restrictive group for unauthorized AP.
clone <source>	Name of an existing AP group from which profile names are copied.
dot11-60GHz-radio-profile <profile-name>	Configures 802.11 60 GHz radio profile. See rf dot11-60GHz-radio-profile on page 1226 .
dot11-6GHz-radio-profile <profile-name>	Configures 802.11 6 GHz radio profile.
dot11a-radio-profile <profile-name>	Configures 802.11a radio settings and load balancing for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 1196 .
dot11a-secondary-radio-profile <profile-name>	Configures 802.11a secondary radio settings and load balancing for the AP group; contains the ARM profile.
dot11a-traffic-mgmt-profile <profile-name>	Configures bandwidth allocation. See wlan traffic-management-profile on page 4204 .

Parameter	Description
<pre>dot11g-radio-profile <profile-name></pre>	<p>Configures 802.11g radio settings and load balancing for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 1196.</p>
<pre>dot11g-traffic-mgmt-profile <profile-name></pre>	<p>Configures bandwidth allocation. See wlan traffic-management-profile on page 4204.</p>
<pre>enet-usb-port-profile default NoAuthWiredPort shutdown <profile-name></pre>	<p>Allows connection of certain devices that use a USB connection as an Ethernet port. This parameter configures the USB port to function as a wired port (downlink), which is governed by AP wired-port profiles.</p> <p>shutdown</p> <p>NOTE: This parameter is not applicable when a USB modem that is connected to an IAP or Remote AP functions as an uplink.</p>
<pre>enet0-port-profile <profile-name></pre>	<p>Configures the duplex and speed of the Ethernet interface 0 on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 415.</p>
<pre>enet1-port-profile <profile-name></pre>	<p>Configures the duplex and speed of the Ethernet interface 1 on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 415.</p>
<pre>enet2-port-profile <profile-name></pre>	<p>Configures the duplex and speed of an Ethernet interface 2 on the AP. These profiles are defined using the command ap wired-port-profile on page 415.</p>
<pre>enet3-port-profile <profile-name></pre>	<p>Configures the duplex and speed of an Ethernet interface 3 on the AP. These profiles are defined using the command ap wired-port-profile on page 415.</p>
<pre>enet4-port-profile <profile-name></pre>	<p>Configures the duplex and speed of an Ethernet 4 interface on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 415.</p>

Parameter	Description
event-thresholds-profile <profile-name>	Configures Received Signal Strength Indication (RSSI) metrics. See rf event-thresholds-profile on page 1245 .
gps-service-profile <profile-name>	Configures GPS service profile.
ids-profile <profile-name>	Configures Aruba's IDS. See ids profile on page 706 .
iot radio-profile <profile-name>	Apply IoT radio profile.
mesh-accesslist-profile	Configures the mesh access list profile.
mesh-cluster-profile <profile-name>	Configures the mesh cluster profile for mesh nodes that are members of the AP group. There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See ap mesh-cluster-profile on page 276 .
priority <1-16>	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The lower the number, the higher the priority. 1-16 1
mesh-radio-profile <profile-name>	Configures the 802.11g and 802.11a radio settings for mesh nodes that are members of the AP group. See ap mesh-ht-ssid-profile on page 279 . Commands to configure mesh for outdoor APs require the Outdoor Mesh license.
no	Negates any configured parameter.
provisioning profile <profile-name>	Configures the provisioning profile.

Parameter	Description
regulatory-domain-profile <profile-name>	Configures the country code and valid channels. See ap regulatory-domain-profile on page 341 .
rf-optimization-profile <profile-name>	Configures coverage hole and interference detection. See rf optimization-profile on page 1252 .
virtual-ap <profile-name>	One or more profiles, each of which configures a specified WLAN. See wlan virtual-ap on page 4210 .
wifi-uplink-profile <wifi-uplink-profile>	Configures a specified Wi-Fi uplink. See ap wifi-uplink-profile on page 407 .
usb-profile <profile-name>	USB profile applied to the AP group.
virtual-ap <profile-name>	One or more profiles, each of which configures a specified WLAN. See wlan virtual-ap on page 4210 .
zigbee service-profile <profile-name>	Apply zigbee related profile.

Example

The following command configures a virtual AP profile to the “default” AP group:

```
(host)[mynode](config) #ap-group test1
(host)[mynode] (AP group "test1") #virtual-ap corpnet
```

The following command configures a Wi-Fi uplink profile to the “default” AP group:

```
(host)[mynode](config)# ap-group wfu-test
Warning: WiFi uplink profile will not take effect until an AP is
reprovisioned
(host)[mynode] (AP group "wfu-test")# wifi-uplink-profile test-uplink
priority 1
```

Related Commands

Command	Description
show ap-group	Shows configuration for an AP group.

Command History

Release	Modification
ArubaOS 8.7.0.0	The following parameters were introduced: <ul style="list-style-type: none">▪ <code>airslice-profile</code>▪ <code>airslice-visibility record-limit</code>▪ <code>mesh-accesslist-profile</code>▪ <code>usb-profile</code>
ArubaOS 8.5.0.0	The following parameters were added: <ul style="list-style-type: none">▪ <code>wifi-uplink-profile</code>▪ <code>enet-usb-port-profile</code>
ArubaOS 8.4.0.0	The <code>dot11-60GHz-radio-profile</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ap image-preload

```
ap image-preload
activate all-aps|specific-aps
add {ap-group <ap-group> | ap-name <ap-name>}
cancel
clear-all
delete {ap-group <ap-group> | ap-name <ap-name>}
[partition <part-num>
[max-downloads <max-downloads>]
```

Description

Configure APs to preload a new software image from a managed device before it starts actively running the new image.

The AP image preload feature minimizes the downtime required for a Mobility Conductor upgrade by allowing the APs to download the new images before the Mobility Conductor actually starts running the new version.

This feature allows you to select the maximum number of APs that are allowed to preload the new software image at any one time, thereby reducing the possibility that the Mobility Conductor may get overloaded or that network traffic may be impacted by all APs on the Mobility Conductor attempting to download a new image at once.

APs can continue normal operation while they are downloading their new software version. When the download completes, the AP sends a message to the Mobility Conductor, informing it that the AP has either successfully downloaded the new software version, or that the preload has failed for some reason. If the download fails, the AP will retry the download after a brief waiting period.

You can allow every AP on a managed device to preload a new software version, or also create a custom list of AP groups or individual APs that can use this feature. If a new AP associates to the managed device while the AP image download feature is active, the managed device will check the name and group of that AP to see if it appears in the preload list. If an AP is on the list, (and does not already have the specified image in its Flash memory) that AP will start preloading its image.

Once a software version has been downloaded by an AP, another version cannot be downloaded until the AP reboots.

Parameter	Description
activate	Activate this feature, allowing APs in the preload list to start downloading their new image from the managed device.
all-aps	All APs will be allowed to pre-download the image.

Parameter	Description
<code>specific-aps</code>	Only APs in the preload list will be allowed to preload the image.
<code>add</code>	Add individual APs or AP groups to the list of APs allowed to preload the image.
<code>ap-group <group></code>	Add a group of APs to the preload list.
<code>ap-name <name></code>	Add an individual AP to the preload list.
<code>cancel</code>	Cancel the AP preload and clear the preload list. Any APs downloading a new image at the time this command is issued will continue to download the file.
<code>clear-all</code>	Clear all APs from the preload list.
<code>delete</code>	Delete an individual AP or AP group from the preload list. This command may be issued before or after preloading is activated. If it is executed after preloading has already been activated, any APs downloading a new image at the time this command is issued will continue to download the file. APs that are still waiting to preload will be removed from the preload list.
<code>ap-group <group></code>	Remove the specified group of APs from the preload list
<code>ap-name <name></code>	Remove an individual AP from the preload list
<code>partition <partition-num></code>	Specify the partition from which the APs should download their images. By default, the APs will preload images from the default boot partition of the managed device.
<code>max-downloads <max-downloads></code>	Specify the maximum number of APs that can simultaneously download their image from the managed device. The default value is ten APs.

Example

The following command enables the image preload feature and adds the APs in the AP groups corp1 and corp2 to the preload list.

```
(host) [mynode] (config) #ap image-preload activate specific-aps
(host) [mynode] (config) #add ap-group corp1
(host) [mynode] (config) #add ap-group corp2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Conductor.

ap-lacp-striping-ip

```
ap-lacp-striping-ip
  aplacp-enable
  no
  striping-ip <ip-addr> lms <LMS>
```

Description

Define an AP LACP LMS map information profile that maps a GRE striping IP address to an existing LMS-IP address.

The **AP LACP LMS map information** profile is a local profile that maps a LMS IP address (defined in the AP system profile) to a GRE striping IP address. If 220 Series or 270 Series access points fail over to a standby or backup controller, the AP LACP LMS map information profile on the new controller defines the IP address that the APs use to terminate 802.11.g radio tunnels on the new controller. This feature allows 220 Series, 270 Series, and 320 Series access points to continue to support link aggregation to a backup controller in the event of a controller failure even if the backup controller is in a different L3 network.



If your topology includes a backup controller you must define GRE striping IP settings in the active and the backup controller.

Parameter	Description
ap-lacp-striping-ip	Configures the AP LACP LMS map information.
aplacp-enable	Enables LACP IP striping. This feature is disabled by default.
no ...	Negate any setting or return a configured parameter to its default value.
striping-ip <ip-addr>	Specify an IPv4 address for the 802.11g radio of the controller to allow LACP-enabled switches to send traffic for the two controller radios on different links. Recommended value for this parameter is lms <ip-addr>+1 .
lms <LMS>	Enter the LMS IP address currently defined in the device's AP system profile to map the existing LMS IP to the GRE striping IP address.

Examples

The following commands enable LACP IP striping on the Mobility Conductor:

```
(host)[node] (config) #ap system-profile LACP
```

```
(host)[node] (AP system-profile "LACP") #lms-ip 192.0.2.1
(host)[node] (AP system-profile "LACP") #bkup-lms-ip 192.0.77.1
(host)[node] (AP system-profile "LACP") #exit
(host)[node] (config) #ap-lacp-striping-ip
(host)[node] (AP LACP LMS map information) #striping-ip 192.0.2.2 lms
192.0.2.1
(host)[node] (AP LACP LMS map information) #aplacp-enable
```

The following commands enable LACP IP striping on an L2-connected High Availability (HA) standby or HA+VRRP controller:

```
(bkup-host)[node] (config) #ap-lacp-striping-ip
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
192.0.2.16 lms 192.0.2.1
(bkup-host) [node] (config)(AP LACP LMS map information) #aplacp-enable
```

The following commands enable LACP IP striping on L3-connected High Availability (HA) standby controllers, or HA controllers in dual HA mode, where each dual-mode controller acts as standby for the APs served by the other dual-mode controller:

```
(bkup-host)[node] (config) #ap-lacp-striping-ip
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
10.1.1.14 lms 192.0.2.1
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
192.0.2.2 lms 192.0.2.1
(bkup-host) [node] (config)(AP LACP LMS map information) #aplacp-enable
```



If you are using High Availability between L3-connected or dual-mode controllers, you must configure **two** different striping IPs (one for each subnet) to ensure that both controllers will have striping IPs mapped to the corresponding LMS IP address.

Important Points to Remember

- In the upstream direction when the AP transmits GRE frames to the Mobility Conductor the bonding driver must be in active-active mode and not in the default active-standby mode to allow link aggregation.
- If an AP's uplink access switch ports are configured in static port-channel mode, then the AP will set the Ethernet bonding mode to static port-channel (xor mode) only if **gre-striping-ip** is configured. If **gre-striping-ip** is not configured, then the AP goes back to **active-standby** mode. In this scenario, the AP may go down depending on the behavior of the upstream switch.
- If an AP's uplink access switch ports are configured in dynamic LACP mode, the AP detects LACP-PDUs and automatically sets the Ethernet bonding mode to LACP. If **gre-striping-ip** is

not configured, then the AP's Ethernet bonding mode will continue to be in LACP mode, but the AP will send GRE traffic only through one Ethernet port.

- In 320 Series and 330 Series access points, if AP uplink packet capture is taken, the downstream traffic will have sequence number in GRE header. Wireshark Aruba wlan decoder will not be able to decode these packets correctly since it looks for known Aruba GRE tunnel IDs.
- Ensure that the **gre-striping-ip** is unique and not used by any other host on the subnet.
- LACP support is limited to a use case where Enet 0 and Enet 1 ports of the AP are connected to a switch, and LACP is enabled on the two corresponding switch ports.
- The port priority is not applicable to the AP as both ports need to be used. This value is always set to the maximum numerical priority (0xFF), which is the lowest priority.
- The system priority is not configurable. It is set to the maximum numerical value (0xFFFF), which is the lowest priority. This leaves control of the aggregate to the upstream switch.
- The timeout value is not configurable.
- The key is not configurable and the default key value is 1.
- LACP cannot be enabled if wired AP functionality is enabled on the second port. You cannot enable LACP if the Enet 1 port is shutdown.

Troubleshooting Link Aggregation

The following show commands in the CLI can be used to troubleshoot Link Aggregation on 220 Series , 270 Series, 320 Series and 330 Series access points:

- `show ap debug lacp ap-name <ap-name>`—Using this command, you can view if LACP is active on an AP. It displays the number of GRE packets sent and received on the two Ethernet ports. Using this command with verbose option on 320 Series and 330 Series access points displays packet re-ordering statistics of each wlan client.
- `show ap database`—The output of this command includes an **LACP Striping** flags to indicate of the AP is configured with a LACP striping IP address,
- `show datapath tunnel`—Using this command on 220 Series/270 Series access points, you can verify if the 2.4GHz tunnels are anchored on the **gre-striping-ip** (The GRE IDs for these tunnels are in a range between 0x8300 and 0x83F0) . On 320 Series and 330 Series access points, use the verbose option to verify that 5 Ghz tunnels have striping IP set in the column **StripIP** (The GRE IDs for these tunnels are in a range between 0x8200 and 0x82F0).
- `show datapath station`—On 320 Series and 330 Series access points, using this command displays the LACP sequence number sent in the GRE header of the last packet to the client. This information is displayed under **Seq** column.
- `show ap remote debug anul-sta-entries`—On 320 Series and 330 Series access points, using this command displays LAG enabled/disabled per station and data drops due to LAG packet reordering.
- `show datapath user`—Using this command, you can verify if the **gre-striping-ip** has an entry with the 'L' (local) flag

- `show datapath route-cache`—Using this command, you can verify if the **gre-striping-ip** has an entry with the LC MAC.

Related Commands

The following show commands display information about the settings defined in the AP LACP LMS map information profile:

Command	Description
show ap-lacp-striping-ip	Displays all settings defined in AP LACP LMS map information profile.
show ap database	The output of this command displays an s flag to indicate that the AP is enabled with a striping IP address.
show ap debug lacp	The output of this command displays the striping IP address of the AP, as defined in the AP LACP LMS map information profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap-leds

ap-leds

```
{all | ap-group <ap-group> | ap-name <ap-name> | ip-addr <ip address> | wired-mac  
<mac address>}
```

Description

This command allows you to make the LEDs on a defined set of APs either blink or display in the currently configured LED operating mode. Note that if the LED operating mode defined in the AP's system profile is set to "off", then the `normal` parameter in the `ap-leds` command will disable the LEDs. If the LED operating mode in the AP system profile is set to "normal" then the `normal` parameter in this command will allow the LEDs light as usual.

Parameter	Description
<code>all</code>	Controls the LED behavior for all APs.
<code>global</code>	Selects all APs on all controllers. <ul style="list-style-type: none">▪ blink: Make LEDs blink for identification.▪ fault-disable: Disable the fault LED if fault is detected. This is applicable for APs with one LED only.▪ fault-enable: Enable the fault LED if fault is detected. This is applicable for APs with one LED only.▪ normal: Restore LEDs to their normal behavior.
<code>local</code>	Selects all APs registered on this controller.
<code>ap-group <ap-group></code>	Controls the LED behavior for APs in the specified group.
<code>ap-name <ap-name></code>	Controls the LED behavior for the AP with the specified name.
<code>ip-addr <ip-addr></code>	Controls the LED behavior for the AP with the specified IP address.
<code>wired-mac <mac-addr></code>	Controls the LED behavior for the AP with the specified MAC address.

Example

The following command causes all local APs to blink their LEDs for identification purposes:

```
(host) [mynode] (config) #ap-leds
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap lldp med-network-policy-profile

```
ap lldp med-network-policy-profile {default | <profile-name>}
  application-type
  guest-voice
  guest-voice-signaling
  softphone-voice
  streaming-video
  video-conferencing
  video-signaling
  voice
  voice-signaling
  clone {default | <source>}
  dscp <dscp>
  l2-priority <l2-priority>
  no ...
  tagged
  vlan <vlan>
```

Description

Define an LLDP MED network policy profile that defines DSCP values and L2 priority levels for a voice or video application.

LLDP-MED (media endpoint devices) is an extension to LLDP that supports interoperability between VoIP devices and other networking clients. LLDP-MED network policy discovery lets endpoints and network devices advertise their VLAN IDs (for example, voice VLAN), priority levels, and DSCP values. ArubaOS supports a maximum of eight LLDP -MED Network Policy profiles.

Creating an LLDP MED network policy profile does not apply the configuration to any AP or AP interface or interface group. To apply the LLDP-MED network policy profile, you must associate it to an LLDP profile, then apply that LLDP profile to an AP wired port profile.

Parameter	Description
ap lldp med-network-policy-profile <profile-name>	Configures an AP LLDP-MED Network Policy Profile. Default
application-type	Specifies the type of application that this profile manages.
guest-voice	Use this application type if the AP services a separate voice network for guest users and visitors.
guest-voice-signaling	Use this application type if the AP is part of a network that requires a different policy for guest voice signaling than for guest voice media. Do not use this application type if both the same network policies apply to both guest voice and guest voice signaling traffic.

Parameter	Description
<code>softphone-voice</code>	Use this application type if the AP supports voice services using soft phone software applications on devices such as PCs or laptops.
<code>streaming-video</code>	Use this application type if the AP supports broadcast or multicast video or other streaming video services that require specific network policy treatment. This application type is not recommended for video applications that rely on TCP with buffering.
<code>video-conferencing</code>	Use this application type if the AP supports video conferencing equipment that provides real-time, interactive video and audio services.
<code>video-signaling</code>	Use this application type if the AP is part of a network that requires a different policy for video signaling than for the video media. Do not use this application type if both the same network policies apply to both video and video signaling traffic.
<code>voice</code>	Use this application type if the AP services IP telephones and other appliances that support interactive voice services. This is the default application type.
<code>voice-signaling</code>	Use this application type if the AP is part of a network that requires a different policy for voice signaling than for the voice media. Do not use this application type if both the same network policies apply to both voice and voice signaling traffic.
<code>clone {default <source>}</code>	Makes a copy of an existing profile by specifying that profile name.
<code>dscp <dscp></code>	Selects a DSCP priority value for the specified application type by specifying a value from 0-63, where 0 is the lowest priority level and 63 is the highest priority. 0-63 0
<code>l2-priority <L2-priority></code>	Select a 802.1p priority level for the specified application type, by specifying a value from 0-7, where 0 is the lowest priority level and 7 is the highest priority. 0-7 0
<code>no</code>	Negates any setting or return a configured parameter to its default value.

Parameter	Description
tagged	Specifies if the policy applies to a to a VLAN that is tagged with a VLAN ID or untagged. The default value is untagged. When an LLDP-MED network policy is defined for use with an untagged VLAN, then the L2 priority field is ignored and only the DSCP value is used. untagged
vlan <vlan>	Specifies a VLAN by VLAN ID (0-4094) or VLAN name. 0

Example

The following commands create a LLDP MED network policy profile for streaming video applications and marks streaming video as high-priority traffic.

```
(host) [mynode] (config) #ap lldp med-network-policy-profile vid-stream
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #dscp 48
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #l2-
priority 6
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #tagged
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #vlan 10
```

Next, the LLDP MED network policy profile is assigned to an LLDP profile, and the LLDP profile is associated with an AP wired-port profile.

```
(host) [mynode] (config) #ap lldp profile video1
(host) [mynode] (AP LLDP Profile "video1") #ap lldp-med-network-policy-
profile vid-stream
(host) [mynode] (AP LLDP Profile "video1") #
(host) [mynode] (config) #ap wired-port-profile corp2
(host) [mynode] (AP wired port profile "corp2") #lldp-profile video1
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap lldp profile

```
ap lldp profile {default | <profile-name>}
  clone {default | <source>}
  dot1-tlvs [port-vlan | vlan-name]
  dot3-tlvs [link-aggregation | mac| mfs| power]
  lldp-med-network-policy-profile {default | <lldp-med-network-policy-profile>}
  lldp-med-tlvs [capabilities | inventory | network-policy]
  no ...
  optional-tlvs [capabilities | management-address | port-description | system-
description | system-name]
  receive
  transmit
  transmit-hold <transmit-hold [1-100]>
  transmit-interval <transmit-interval[1-3600]>
```

Description

Define an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

LLDP is a Layer-2 protocol that allows network devices to advertise their identity and capabilities on a LAN. Wired interfaces on Aruba APs support LLDP by periodically transmitting LLDP PDUs consisting of TLV elements. Use this command to specify the TLV that should be sent by the AP interface associated with the LLDP profile.

Parameter	Description
ap lldp profile <profile-name>	Configures an AP LLDP profile. default
clone <profile>	Make a copy of an existing LLDP profile. default
dot1-tlvs	Specify the 802.1 TLV that the AP will send in LLDP PDUs. By default, the AP will send every 802.1 TLV.
port-vlan	Transmit the LLDP 802.1 port VLAN TLV. If the native VLAN is configured on the port, the port-vlan TLV will send that value, otherwise it will send a value of 0.
vlan-name	Transmit the LLDP 802.1 VLAN name TLV. The AP sends a value of "Unknown" for VLAN 0, or "VLAN <number>" for non-zero VLAN numbers.
dot3-tlvs	Specify the 802.3 TLV that the AP will send in LLDP PDUs. By default, the AP will send every 802.3 TLV.
link-aggregation	Transmit the 802.3 link aggregation TLV to indicate that link aggregation is not supported.

Parameter	Description
mac	Transmit the 802.3 MAC or PHY Configuration or Status TLV to indicate the duplex and bit rate capacity, and current duplex and bit rate settings of the AP interface.
mfs	Transmit the 802.3 Maximum Frame Size TLV to show the maximum frame size capability of the AP.
power	Transmit the 802.3 Power via media dependent interface (MDI) TLV to show the power support capabilities of the AP interface. This parameter is supported by the RAP-3WNP and 130 Series only.
lldp-med-network-policy-profile <profile>	Specify the LLDP MED Network Policy profile to be associated with this LLDP profile.
lldp-med-tlvs	Specify the LLDP-MED TLV that the AP will send in LLDP PDUs. By default, the AP will not send any LLDP-MED TLV.
capabilities	Transmit the LLDP-MED capabilities TLV. The AP will automatically send this TLV if any other LLDP-MED TLV is enabled.
inventory	Transmit the LLDP-MED inventory TLV. An AP cannot send this TLV unless it also sends the LLDP-MED capabilities TLV.
network-policy	Transmit the LLDP-MED network-policy TLV. An AP cannot send this TLV unless it also sends the LLDP-MED capabilities TLV.
optional-tlvs	Specify the optional TLV that the AP will send in LLDP PDUs.
capabilities	Transmit the system capabilities TLV to indicate which capabilities are supported by the AP.
management-address	Transmit a TLV that indicates the management IP address of the AP, in either IPv4 or IPv6 format.
port-description	Transmit a TLV that gives a description of the wired port of an AP in an alphanumeric format.
system-description	Transmit a TLV that describes the model number and software version of the AP.
system-name	Transmit a TLV that sends the AP name or wired MAC address.
receive	Issue this command to enable LLDP PDU reception. This parameter is enabled by default.

Parameter	Description
transmit	Issue this command to enable LLDP PDU transmission. This parameter is enabled by default.
transmit-hold <transmit-hold>	Enter a value from 1-100. This value is multiplied by the transmit interval to determine the number of seconds to cache learned LLDP information before that information is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then learned LLDP information will be cached for 4 x 30 seconds, or 120 seconds. 1-100 4
transmit-interval <transmit-interval>	The interval between LLDP TLV transmission seconds. The supported range is 1-3600 seconds and the default value is 30 seconds. 1-3600 30

Example

The following command configures an LLDP profile, allows the AP interface to send the port-vlan and vlan-name TLV.

```
(host) [mynode] (config)#ap lldp profile 8021TLVs
(host) [mynode] (AP LLDP Profile "8021TLVs") #dot1-tlvs port-vlan
(host) [mynode] (AP LLDP Profile "8021TLVs") #dot1-tlvs vlan-name
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

```

ap mesh-accesslist-profile <name>
  ap-name <ap-name>
  type [allow | deny]
  clone <source>
  no

```

Description

This command configures a mesh access list profile. Mesh access list profile defines the list of APs each AP is allowed to discover in a mesh topology.

Parameter	Description
ap mesh-accesslist-profile <name>	Defines the name of the mesh access list profile.
ap-name <ap-name>	APs that are either allowed or denied to be discovered.
type	Allows or Denies APs to be discovered.
allow	Allows the APs in the list to be discovered. All other APs not in the list will be denied.
deny	APs in the list will not be discovered. All other APs not in the list will be allowed.
clone <source>	Copies data from a different mesh access list profile.
no	Deletes the profile.

The mesh access list profile is associated to an AP group or an AP using the following commands:

```

(host) [mynode] (config) #ap-group default
(host) [mynode] (AP group "default") #mesh-accesslist-profile Guest
(host) [mynode] (config) #ap-name AP-505
(host) [mynode] (AP name "AP-505") #mesh-accesslist-profile Guest

```

Example

The following commands configure a mesh access list profile:

```

(host) [mynode] (config) #ap mesh-accesslist-profile Guest
(host) [mynode] (Mesh Accesslist profile "Guest") #ap-name lab-1
(host) [mynode] (Mesh Accesslist profile "Guest") #ap-name AP-303
(host) [mynode] (Mesh Accesslist profile "Guest") #ap-name AP-3034
(host) [mynode] (Mesh Accesslist profile "Guest") #type allow

```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap mesh-cluster-profile

```
ap mesh-cluster-profile <profile-name>
  clone <source>
  cluster <cluster>
  no
  opmode {opensystem|wpa2-psk-aes}
  rf-band {a|g|all}
  rf-split5G-band-range { first | full | lower |upper }
  wpa-hexkey <wpa-hexkey>
  wpa-passphrase <wpa-passphrase>
```

Description

Mesh cluster profiles are specific to mesh nodes (APs configured for mesh) and provide the framework of the mesh network. You must define and configure the mesh cluster profile before configuring an AP to operate as a mesh node.

You can configure multiple mesh cluster profiles to be used within a mesh cluster. You must configure different priority levels for each mesh cluster profile. See [ap-group](#) or [ap-name](#) for more information about priorities.

Cluster profiles, including the default profile, are not applied until you provision your APs for mesh.

Parameter	Description
ap mesh-cluster-profile <profile-name>	Configures a mesh cluster profile. Give a name to the mesh cluster profile. The name must be 1–63 characters long.
clone <source>	Copies parameter values from an existing mesh cluster profile.
cluster <cluster>	Indicates the mesh cluster name. The name can have a maximum of 32 characters and is used as the MSSID for the mesh cluster. When you first create a new mesh cluster profile, the profile uses the default cluster name “Aruba-mesh”. Use the <code>cluster</code> parameter to define a new, unique MSSID before you assign APs or AP groups to the mesh cluster profile. If you want a mesh cluster to use WPA2-PSK-AES encryption, <i>do not use spaces in the mesh cluster name</i> , as this may cause errors in mesh points associated with that mesh cluster.
no	Negates any configured parameter.
opmode	Configures one of the following data encryption types: <ul style="list-style-type: none">■ opensystem: No encryption.■ wpa2-psk-aes: WPA2 with AES encryption using a pre-shared key.

Parameter	Description
	<p>Best practices are to select wpa2-psk-aes and use the <code>wpa-passphrase</code> parameter to select a passphrase. Keep the passphrase in a safe place.</p> <p>opensystem, wpa2-psk-aes</p> <p>opensystem</p>
<code>rf-band</code>	<p>Configures the RF band in which multiband mesh nodes must operate:</p> <ul style="list-style-type: none"> ■ a: 802.11a ■ g: 802.11g ■ all: all bands. Mesh feature will be enabled on both a and g bands. <p>Best practices are to use 802.11a radios for mesh deployments.</p> <p>a</p>
<code>rf-split5G-band-range</code>	<p>This command configures the 5 GHz radio used for the mesh link. This parameter takes effect only when split 5 GHz or dual 5 GHz radio is enabled on the AP. Reboot the AP must for the configuration to take effect.</p>
<code>first</code>	<p>Configures the functioning 5 GHz radio as the mesh link.</p>
<code>full</code>	<p>Configures both the sub bands of the 5 GHz radio as the mesh link. The radio assignment however depends on factors such as hopcount to the mesh portal, availability of neighboring mesh APs, and preferred uplink radio setting of the mesh profile. This is the default setting.</p>
<code>lower</code>	<p>Configures the lower 5 GHz radio as the mesh link.</p>
<code>upper</code>	<p>Configures the upper 5 GHz radio as the mesh link.</p>
<code>wpa-hexkey <wpa-hexkey></code>	<p>Configures a WPA PSK.</p>
<code>wpa-passphrase <wpa-passphrase></code>	<p>Sets the WPA password that generates the PSK.</p>

Example

The following command configures a mesh cluster profile named `cluster1`, for the mesh cluster headquarters:

```
(host) [mynode] (config) #ap mesh-cluster-profile cluster1
(host) [mynode] (Mesh Cluster profile "cluster1")cluster headquarters
```

Related Commands

Command	Description
show ap mesh-cluster-profile	Displays the complete list of cluster profiles and their profile status. Include the <profile-name> parameter to view the settings for a specific mesh cluster profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>rf-band all</code> and <code>rf-split5G-band-range</code> parameters were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap mesh-ht-ssid-profile

```
ap mesh-ht-ssid-profile {default | <profile-name>}
  40MHz-enable
  80MHz-enable
  ba-amsdu-enable
  clone {default | <source>}
  high-efficiency-enable
  high-throughput-enable
  ldpc
  legacy-stations
  max-rx-a-mpdu-size {8191 | 16383 | 32767 | 65535}
  max-tx-a-mpdu-size <max-tx-a-mpdu-size>
  max-tx-a-msdu-count-be <max-tx-a-msdu-count-be>
  max-tx-a-msdu-count-bk <max-tx-a-msdu-count-bk>
  max-tx-a-msdu-count-vi <max-tx-a-msdu-count-vi>
  max-tx-a-msdu-count-vo <max-tx-a-msdu-count-vo>
  max-vht-mpdu-size {3895 | 7991 | 11454}
  min-mpdu-start-spacing {0.25 | 0.5 | 0 | 1 | 2 | 4 | 8 | 16}
  mpdu-agg
  no
  short-guard-intvl-20MHz
  short-guard-intvl-40MHz
  short-guard-intvl-80MHz
  stbc-rx-streams {0 | 1}
  stbc-tx-streams
  supported-mcs-set
  temporal-diversity
  very-high-throughput-enable
  vht-supported-mcs-map <supported-mcs-set>
  vht-txbf-explicit-enable
```

Description

The mesh HT SSID profile defines settings unique to 802.11n-capable, high-throughput APs. If none of the APs in your mesh deployment are 802.11n-capable APs, you do not need to configure a HT SSID profile.

If you modify a currently provisioned and running high-throughput SSID profile, your changes take effect immediately. You do not reboot the Mobility Conductor or the AP.

Parameter	Description
ap mesh-ht-ssid-profile <profile-name>	Configures a Mesh HT SSID profile. Enter the name of an existing mesh high-throughput SSID profile to modify that profile, or enter a new name or create a new mesh HT profile. The mesh HT profile can have a maximum of 32 characters.

Parameter	Description
	To view existing HT SSID radio profiles, use the command <code>show ap mesh-radio-profile</code> . default
40MHz-enable	Enable or disable the use of 40 MHz channels. enabled
80MHz-enable	Enable or disable the use of 80 MHz channels. enabled
ba-amsdu-enable	Enable or Disable Receive AMSDU in BA negotiation. enabled
clone <source>	Copy configuration information from a source profile into the currently selected profile.
high-efficiency-enable	Enables high-efficiency (802.11ax) features on this SSID.
high-throughput-enable	Enable or disable HT (802.11n) features on this SSID. enabled
ldpc	If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise. enabled
legacy-stations	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed). enabled
max-rx-a-mpdu-size	Maximum size of a received aggregate MPDU, in bytes. 8191, 16383, 32767, 65535
max-tx-a-mpdu-size <max-tx-a-mpdu-size>	Maximum size of a transmitted aggregate MPDU, in bytes. 1576-65535
max-tx-a-msdu-count-be <max-tx-a-msdu-count-be>	Maximum number of MSDUs in a TX A-MSDU on best-effort AC. TX-AMSDU disabled if 0. 0-15 2
max-tx-a-msdu-count-bk <max-tx-a-msdu-count-bk>	Maximum number of MSDUs in a TX A-MSDU on background AC. TX-AMSDU disabled if 0.

Parameter	Description
	0-15 2
max-tx-a-msdu-count-vi <max-tx-a-msdu-count-vi>	Maximum number of MSDUs in a TX A-MSDU on video AC. TX-AMSDU disabled if 0. 0-15 2
max-tx-a-msdu-count-vo <max-tx-a-msdu-count-vo>	Maximum number of MSDUs in a TX A-MSDU on voice AC. TX-AMSDU disabled if 0. 0-15 0
max-vht-mpdu-size	Maximum size of a VHT MPDU. 3895, 7991, 11454 11454
min-mpdu-start-spacing	Minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds. 0, 0.25, 0.5, 1, 2, 4, 8, 16 0
mpdu-agg	Enable or disable MPDU aggregation. HT mesh APs are able to send aggregated MPDUs, which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU. enabled
no	Delete command.
short-guard-intvl-20Mhz	Enable or disable use of short (400 ns) guard interval for 130 Series APs in 20 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.

Parameter	Description
	enabled
short-guard-intvl-40Mhz	<p>Enable or disable use of short (400 ns) guard interval in 40 MHz mode.</p> <p>A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data.</p> <p>The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>enabled</p>
short-guard-intvl-80Mhz	<p>Enable or disable use of short (400 ns) guard interval in 80 MHz mode.</p> <p>A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data.</p> <p>The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>enabled</p>
stbc-rx-streams	<p>Controls the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)</p> <p>0-1 1</p>
stbc-tx-streams	<p>Controls the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on 170 Series, 130 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)</p>

Parameter	Description
	0-1 1
supported-mcs-set <supported-mcs-set>	A list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz) and the number of spatial streams used by the mesh node. The default value is 0-31—16-23 are supported on 130 Series/RAP-15x/802.11ac APs only; 24-31 are supported on 320 Series/330 Series only. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma. 0-31 0-31
temporal-diversity	Shows if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries. disabled
very-high-throughput-enable	Shows if very-high-throughput (802.11ac) features are enabled or disabled. enabled
vht-supported-mcs-map <supported-mcs-set>	Comma-separated list of max supported MCS for spatial streams 1 through 4. Valid values for max MCS are 7, 8, 9, and - (if spatial stream is not supported). Max MCS of a spatial stream cannot be higher than the MCS of the previous stream. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx. 9,9,9,9
vht-txbf-explicit-enable	Enable or Disable use of VHT Explicit Transmit Beamforming. enabled

Example

The following command configures a mesh HT SSID profile named “HT1” and sets some non-default settings for MPDU aggregation:

```
(host) [mynode] (config) #ap mesh-ht-ssid-profile HT1
```

```
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #max-rx-a-mpdu-size 32767
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #max-tx-a-mpdu-size 32767
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #min-mpdu-start-spacing .25
```

Related Commands

Command	Description
show ap mesh-ht-ssid-profile	View a complete list of mesh HT SSID profiles and their status.
show ap mesh-ht-ssid-profile	View the settings of a specific mesh radio profile.

Command History

Release	Modification
ArubaOS 8.6.0.0	The <code>high-efficiency-enable</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap mesh-radio-profile

```
ap mesh-radio-profile {default | <profile-name>}
  a-tx rates [6 | 9 | 12 | 18 | 24 | 36 | 48 | 54]
  allowed-vlans <vlan-list>
  children <children>
  clone {default | <source>}
  eapol-rate-opt
  g-tx rates [1 | 2 | 5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54]
  heartbeat-threshold <heartbeat-threshold>
  hop-count <hop-count>
  link-threshold <link-threshold>
  max-retries <max-retries>
  mesh-ht-ssid-profile {default | <profile-name>}
  mesh-mcast-opt
  mesh-mobility
  mesh-survivability
  metric-algorithm {best-link-rssi | distributed-tree-rssi}
  mobility-beacon-miss <mobility-beacon-miss>
  mobility-rssi <mobility-rssi>
  mpv <mpv>
  no ...
  optimize-scan-interval
  prefer-uplink-radio {2g | 5g | 5g-lower | 5g-upper | 6GHz | none}
  reselection-mode {reselect-anytime | reselect-never | startup-subthreshold |
  subthreshold-only}
  rts-threshold <rts-threshold>
```

Description

Mesh radio profiles are specific to mesh nodes (APs configured for mesh) and determine the RF or channel used by mesh nodes to establish mesh links and the path to the mesh portal. You can configure multiple radio profiles; however, you select and deploy only one radio profile per mesh cluster.

Radio profiles, including the “default” profile, are not active until you provision your APs for mesh. If you modify a currently provisioned and running radio profile, your changes take place immediately. You do not reboot the Mobility Conductor or the AP.

Parameter	Description
ap mesh-radio-profile <profile>	Configures a Mesh Radio profile. Give a name to this instance of the profile. The name must be 1–63 characters long.

Parameter	Description
	default
a-tx rates	<p>Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.</p> <p>6, 9, 12, 18, 24, 36, 48, 54</p>
allowed-vlans	<p>Specifies a list of VLAN IDs that can be used by a mesh link on APs associated with this mesh radio profile</p>
<vlan-list>	<p>A comma-separated list of VLAN IDs. You can also specify a range of VLAN IDs using a dash (for example, 1-4095)</p>
children <children>	<p>Indicates the maximum number of children a mesh node can accept.</p> <p>1-64 64</p>

Parameter	Description
clone <source>	<p>Name of an existing mesh radio profile from which parameter values are copied.</p> <p>default</p>
eapol-rate-opt	<p>Use a more conservative rate for more reliable delivery of EAPOL frames.</p> <p>disabled</p>
g-tx rates	<p>Indicates the transmit rates for the 802.11b or 802.11g radio.</p> <p>The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.</p> <p>1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54</p>
heartbeat-threshold <heartbeat-threshold>	<p>Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes.</p> <p>1-255</p> <p>30</p>

Parameter	Description
<pre>hop-count <hop-count></pre>	<p>Indicates the maximum hop count from the mesh portal.</p> <p>1-32</p> <p>8</p>
<pre>link-threshold <link-threshold></pre>	<p>Indicates the minimal RSSI value. If the RSSI value is below this threshold, the link may be considered a sub-threshold link. A sub-threshold link is a link whose average RSSI value falls below the configured threshold. If this occurs, the mesh node may try to find a better link on the same channel and cluster (only neighbors on the same channel are considered). The supported threshold is hardware dependent, with a practical range of 10-90.</p> <p>12</p>
<pre>max-retries <max-retries></pre>	<p>Maximum number of times a mesh node can re-send a packet.</p> <p>0-15</p> <p>4</p>

Parameter	Description
<pre>mesh-ht-ssid-profile <profile-name></pre>	<p>HT SSID Profile for the mesh feature.</p> <p>default</p>
<pre>mesh-mcast-opt</pre>	<p>Enables or disables scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children. Best practices are to use the default value.</p> <p>enabled</p>
<pre>mesh-mobility</pre>	<p>Enables fast roaming on a mobility mesh point based on low RSSI or missed beacon frames.</p> <p>disabled</p>

Parameter	Description
<code>mesh-survivability</code>	<p>Allows mesh points and portals to become active even if the Mobility Conductor cannot be reached by bridging LAN traffic. This is a beta feature that is disabled by default; it should not be enabled unless you are instructed to do so by Aruba technical support.</p> <p>distributed-tree-rssi</p>
<code>metric-algorithm</code>	<p>Specifies the algorithm used by a mesh node to select its parent.</p> <p>distributed-tree-rssi</p>
<code>mobility-beacon-miss</code> <mobility-beacon-miss>	<p>Triggers fast roaming on a mobility mesh point when number of consecutive missed beacon frames reaches the threshold value.</p> <p>10-25</p> <p>16</p>
<code>mobility-rssi</code> <mobility-rssi>	<p>Triggers fast roaming on a mobility mesh point when RSSI of the parent is lower than the threshold value.</p>

Parameter	Description
	10-50 15
best-link-rssi	Selects the parent with the strongest RSSI, regardless of the number of children a potential parent has.
distributed-tree-rssi	Selects the parent based on link-RSSI and node cost based on the number of children. This option evenly distributes the mesh points over high quality uplinks. Low quality uplinks are selected as a last resort.
mpv <mpv>	This parameter is experimental and reserved for future use. 0-4094 0
no	Negates any configured parameter.
optimize-scan-interval	Configures the time period to perform mesh scanning. Range: 1 to 100 hours Default: 24 hours

Parameter	Description
prefer-uplink-radio	Configures the preferred 5 GHz radio for mesh links. Mesh link neighbors identified in this radio band will be prioritized over other neighbors identified in other radio band. This parameter will take effect only when dual 5 GHz or split 5 GHz radio is enabled on the AP and when rf-split5G-band-range is set to full.
2g	Configures 2.4G radio band as preferred uplink.
5g	Configures 5G radio band as preferred uplink.
5g-lower	Configures 5G radio band as preferred uplink.
5g-upper	Configures 5G radio band as preferred uplink .
6GHz versions)	<p data-bbox="708 1541 1052 1566">ArubaOS 8.9.0.0 or later</p> <p data-bbox="1214 1514 1393 1623">Configures 6 GHz radio band as preferred uplink .</p> <p data-bbox="1214 1654 1393 1764">NOTE: This sub-parameter is applicable to Wi-Fi 6E APs</p>

Parameter	Description
	only.
none	Does not specify any radio band as preferred uplink .
reselection-mode	Specifies the method used to find a better mesh link. Best practices are to use the default value startup-subthreshold. start-subthreshold
reselect-anytime	Starting from ArubaOS 8.8.0.0, mesh points using the reselect-anytime reselection mode will perform periodically triggered optimize scanning. This time period is defined using the optimize-scan-interval parameter. If no better parent is found, the mesh point returns to its original parent.

Parameter	Description
	<p>This initial scan first evaluates more distant mesh points before evaluating closer mesh points, and incurs a dropout of 5-8 seconds for each mesh point.</p> <p>Prior to ArubaOS 8.8.0.0, Mesh points using the reselect-anytime reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent.</p> <p>This initial scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5-8 seconds for each mesh point.</p>

Parameter	Description
	After the initial startup scan is completed, connected mesh nodes evaluate mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal.
reselect-never	Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal.

Parameter	Description
startup-subthreshold	<p>Mesh points using the startup-subthreshold reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent. This initial startup scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5–8 seconds for each mesh point. After that time, each mesh node evaluates alternative links if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). Best practices are to use the default startup-subthreshold value.</p>

Parameter	Description
	<p>If a mesh point using the startup-subthreshold mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier distance (or less) with good link quality.</p> <p>For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.</p>

Parameter	Description
subthreshold-only	<p>Starting from ArubaOS 8.8.0.0, the connected mesh nodes evaluate alternative links only if the signal strength of the existing uplink is lesser than the signal strength of link threshold.</p> <p>Prior to ArubaOS 8.8.0.0, Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.</p>

Parameter	Description
	<p>Starting with ArubaOS 3.4.1, if a mesh point using the subthreshold-only mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier distance (or less) with good link quality. For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.</p>

Parameter	Description
<code>rts-threshold</code> <code><rts-threshold></code>	Defines the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue RTS and wait for other mesh nodes to respond with CTS to begin transmission. This helps prevent mid-air collisions. 256-2346 2333

Example

The following example creates a mesh radio profile named "radio2" and associates a mesh HT profile named meshHT1.

```
(host) [mynode] (config) #ap mesh-radio-profile radio2
(host) [mynode] (Mesh Radio profile "radio2") #mesh-ht-ssid-profile meshHT1
```

The following example configures fast roaming on a mobility mesh point.

```
(host) [mynode] (config) #ap mesh-radio-profile mesh_radio_roaming
(host) [mynode] (Mesh Radio profile "mesh_radio_roaming") #mesh mobility
(host) [mynode] (Mesh Radio profile "mesh_radio_roaming") #mobility-rssi 20
(host) [mynode] (Mesh Radio profile "mesh_radio_roaming") #mobility-beacon-miss 10
```

The following example configures 6 GHz radio band on the mesh node for AP-635 access point (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #ap mesh-radio-profile default
(host) [mynode] (Mesh Radio profile "default") #prefer-uplink-radio 6GHz
```

Related Commands

Command	Description
<code>show ap mesh-radio-profile</code>	To view the settings of a specific mesh radio profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	The 6GHz sub-parameter under prefer-uplink-radio parameter was introduced.
ArubaOS 8.8.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The optimize-scan-interval parameter was introduced. ■ The functionality of reselect-any-time and subthreshold-only reselection-modes were changed. ■ The mesh-mobility, mobility-beacon-miss <mobility-beacon-miss>, and mobility-rssi <mobility-rssi> parameters were introduced.
ArubaOS 8.7.0.0	The prefer-uplink-radio parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap modem

```

ap modem
  upgrade <all-aps>|<specific-aps>
  activate
    max-downloads <max-downloads>
  server
    ftp {username <username>|<hostname>}|
    http {username <username>|<hostname>}|
    https {username <username>|<hostname>}|
    scp {username <username>|<hostname>}|
    tftp <hostname>

```

Description

This command upgrades the firmware version of Aruba AP USB LTE modem from the managed device. The managed device first downloads the modem firmware, and then the Remote AP downloads the firmware from the managed device.

Parameter	Description
<code>upgrade <all-aps> <specific-aps></code>	Upgrades modem firmware for all registered APs or the APs specified by ap-group or ap-name.
<code>activate</code>	Downloads modem firmware from activate.
<code>max-downloads <max-downloads></code>	Specify how many applications can download modem firmware at the same time. The default value is 10.
<code>server</code>	Downloads modem firmware from the local server.
<code>ftp {username <username> <hostname>}</code>	Downloads modem firmware from the FTP server.
<code>http {username <username> <hostname>}</code>	Downloads modem firmware from the HTTP server.
<code>https {username <username> <hostname>}</code>	Downloads modem firmware from the HTTPS server.
<code>scp {username <username> <hostname>}</code>	Downloads modem firmware from the SCP server.
<code>tftp <hostname></code>	Downloads modem firmware from the TFTP server.

Example

The following example upgrades modem firmware from the TFTP server for all registered APs.

```
(host) [mynode] #ap modem upgrade all-aps tftp 144.37.254.3 ArubaOS_90xx_
lte_fw_v20_77807
```

Related Command

Command	Description
ap modem-upgrade	This command configures the firmware upgrade of Aruba USB LTE modem.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

ap modem-upgrade

```
ap modem-upgrade
    {activate | add <ap-group|ap-name>| clear-specific-list | delete <ap-
group|ap-name>| reset}
```

Description

This command configures the firmware upgrade of Aruba USB LTE modem, and decides which AP gets upgraded when you issue the `ap modem upgrade <specific-aps>` command. You can add or remove specific AP name or AP group, as well as remove all the AP names and AP groups from the list for modem firmware upgrade. You can also reset the entire firmware upgrade before initiating a new upgrade.

Parameter	Description
<code>activate {disable enable}</code>	Disable or enable automatical upgrade from activate.
<code>add [ap-group <ap-group> ap-name <ap-name>]</code>	Adds AP group or AP name to the list for modem firmware upgrade.
<code>clear-specific-list</code>	Removes all AP groups and AP names from list for modem upgrade.
<code>delete [ap-group <ap-group> ap-name <ap-name>]</code>	Deletes AP group or AP name from list for modem upgrade.
<code>reset</code>	Resets the existing modem firmware upgrade.

Parameter	Description
	<p>This parameter resets the entire upgrade process before a new upgrade is initiated. Hence, you must issue the <code>ap modem-upgrade reset</code> command between two firmware upgrade processes.</p> <p>NOTE: This parameter does not interrupt or cancel the existing firmware download on APs.</p>

Example

The following example removes the AP name from the list for modem firmware upgrade.

```
(host) [mynode] #ap modem-upgrade delete ap-name test
```

Related Command

Command	Description
ap modem	This command upgrades the firmware version of Aruba AP USB LTE modem.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

ap multizone-profile

```
ap multizone-profile <profile-name>
  clone <source>
  datazone <zone>
    controller-ip <ipv4>
    controller-ipv6 <ipv6>
    description <description>
    max-nodes <num_nodes>
    max-vaps <num_nodes>
  multizone-enable
  no
  primaryzone
    max-nodes <num_nodes>
    max-vaps <num_nodes>
```

Description

MultiZone feature allows AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain. The zone can have a single managed device or a cluster. This command allows you to create an AP MultiZone profile, set the data zone index, and controller-ip.

Parameter	Description
<profile-name>	Name of the profile.
clone	Copy data from one AP MultiZone profile to another.
datazone	Data zone Index [1 - 4].
controller-ip <ipv4>	The IPv4 address of the managed device to be configured on one of the data zones.
controller-ipv6 <ipv6>	The IPv6 address of the managed device to be configured on one of the data zones.
description <description>	The description of the data zone. The range of the string is 1-32.
max-nodes <num_nodes>	(Optional) The maximum number of managed devices allowed for the data zone. The range should be between 1 - 11, as the primary zone must have at least one managed device. Default value is 1.
max-vaps <num_vaps>	(Optional) The maximum number of ESSIDs allowed for the data zone. The range should be between 1 - 16. Default value is 3.

Parameter	Description
<code>multizone-enable</code>	If enabled, AP enters MultiZone mode. Default value is disabled.
<code>no</code>	Delete command.
<code>primaryzone</code>	This parameter is used to configure the primary zone.
<code>max-nodes <num_nodes></code>	(Optional) The maximum number of managed devices allowed for the primary zone. The range should be between 1 - 11, as the primary zone must have at least one managed device. Default value is 1.
<code>max-vaps <num_vaps></code>	(Optional) The maximum number of ESSIDs allowed for the primary zone. The range should be between 1 - 16. Default value is 3.

Example

The following command enables AP MultiZone:

```
(host) [mynode] (config) #ap multizone-profile <default> multizone-enable
```

The following command configures IPv6 address of the managed device and sets maximum number of managed devices and ESSIDs on the data zone:

```
(host) [mynode] (config) (ap multizone-profile <default>)# datazone 1
controller-ipv6 2001:1001::201 max-nodes 2 max-vaps 3
```

Command History

Release	Modification
ArubaOS 8.4.0.0	<p>The following sub-parameters were introduced in the <code>datazone</code> parameter:</p> <ul style="list-style-type: none"> ■ <code>controller-ipv6 <ipv6></code> ■ <code>description <description></code> ■ <code>max-nodes <num_nodes></code> ■ <code>max-vaps <num_vaps></code> <p>The following sub-parameters were introduced in the <code>primaryzone</code> parameter:</p> <ul style="list-style-type: none"> ■ <code>max-nodes <num_nodes></code> ■ <code>max-vaps <num_vaps></code>

Release	Modification
ArubaOS 8.1.0.0	The <code>primaryzone</code> parameter was added.
ArubaOS 8.0.1.0	The <code>num-nodes</code> sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

apmove

```
apmove
  all
  ap-group <ap-group>
  ap-mac <ap-mac>
```

Description

When HA is enabled, use this command to move an AP or group of APs to their managed devices. This command should be used when it is necessary to move a single AP, all APs in an ap-group, or all APs to switchover to their standby managed device without an actual failure of the active managed device. For example, this allows the network admin to manually move one or more APs to their managed device and perform a planned upgrade or maintenance on the active managed device.

Parameter	Description
all	Move all APs.
ap-group <ap-group>	Move all APs belonging to the specified AP group.
ap-mac <ap-mac>	Move all APs belonging to the MAC of the specified AP.
target-v4	Target managed device IPv4 address.
target-v6	Target managed device IPv6 address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Config mode on Mobility Conductor.

ap-name

```
ap-name <profile-name>
  airslice-profile <name>
  am-filter-profile {default | <profile-name>}
  ap-multizone-profile {default | <profile-name>}
  ap-system-profile {default | <profile-name>}
  authorization-profile {default | <profile-name>}
  clone {default | <source>}
  dot11-60GHz-radio-profile {default | <profile-name>}
  dot11-6GHz-radio-profile {default | <profile-name>}
  dot11a-radio-profile {default | <profile-name>}
  dot11a-secondary-radio-profile {default | <profile-name>}
  dot11a-traffic-mgmt-profile {default | <profile-name>}
  dot11g-radio-profile {default | <profile-name>}
  dot11g-traffic-mgmt-profile {default | <profile-name>}
  enet0-profile {default | <profile-name>}
  enet1-profile {default | <profile-name>}
  enet2-profile {default | <profile-name>}
  enet3-profile {default | <profile-name>}
  enet4-profile {default | <profile-name>}
  event-thresholds-profile {default | <profile-name>}
  exclude-mesh-cluster-profile-ap {default | <profile-name>}
  exclude-virtual-ap {default | <profile-name>}
  exclude-wifi-uplink-profile {default | <profile-name>}
  gps-service-profile {default | <profile-name>}
  ids-profile {default | <profile-name>}
  iot radio-profile <profile-name>
  mesh-accesslist-profile {default | <profile-name>}
  mesh-cluster-profile {default | <mesh-cluster-profile>} priority <priority>
  mesh-radio-profile {default | <profile-name>}
  no
  regulatory-domain-profile {default | <profile-name>}
  regulatory-domain-profile {default | <profile-name>}
  rf-optimization-profile {default | <profile-name>}
  usb-profile {default | <profile-name>}
  virtual-ap {default | <profile-name>}
  wifi-uplink-profile {default | <profile-name>}
  zigbee service-profile <profile-name>
```

Description

This command configures a specific AP. Profiles that are applied to an AP group can be overridden on a per-AP name basis, and virtual APs can be added or excluded on a per-AP name basis. If a particular profile is overridden for an AP, all parameters from the overriding profile are used. There is no merging of individual parameters between the AP and the AP group to which the AP belongs.

Parameter	Description
ap-name <profile-name>	<p>Configures an AP name. Give a name that identifies the AP. By default, the name of an AP can either be its Ethernet MAC address, or if the AP has been previously provisioned with an earlier version of ArubaOS, a name in the format <building>.<floor>.<location>. The name must be 1-63 characters long.</p> <p>NOTE: You cannot use quotes (") in the AP name.</p>
airslice-profile <name>	Configures an Air Slice profile.
am-filter-profile <profile-name>	Configures AM filter profile.
am-multizone-profile <profile-name>	Configures AP MultiZone profile.
ap-system-profile <profile-name>	Configures AP administrative operations, such as logging levels. See ap system-profile on page 354 .
authorization-profile <profile-name>	Restrictive group for unauthorized AP.
clone <source>	Name of an existing AP name from which profile names are copied.
dot11-60GHz-radio-profile <profile-name>	Configures 802.11 60GHz radio settings for the AP group; contains the ARM profile.
dot11-6GHz-radio-profile <profile-name>	Configures 802.11 6GHz radio settings for the AP group; contains the ARM profile.
dot11a-radio-profile <profile-name>	Configures 802.11a radio settings for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 1196 .
dot11a-secondary-radio-profile <profile-name>	Configures 802.11a secondary radio settings for the AP group; contains the ARM profile.
dot11a-traffic-mgmt-profile <profile-name>	Configures bandwidth allocation. See wlan traffic-management-profile on page 4204 .

Parameter	Description
dot11g-radio-profile <profile-name>	Configures 802.11g radio settings for the AP group; contains the ARM profile. See rf dot11g-radio-profile on page 1228 .
dot11g-traffic-mgmt-profile <profile-name>	Configures bandwidth allocation. See wlan traffic-management-profile on page 4204 .
enet0-profile <profile-name>	Configures the duplex and speed of the Ethernet 0 interface on the AP. See ap enet-link-profile on page 241 .
enet1-profile <profile-name>	Configures the duplex and speed of the Ethernet 1 interface on the AP. See ap enet-link-profile on page 241 .
enet2-profile <profile-name>	Configures the duplex and speed of the Ethernet 2 interface on the AP. See ap enet-link-profile on page 241 .
enet3-profile <profile-name>	Configures the duplex and speed of the Ethernet 3 interface on the AP. See ap enet-link-profile on page 241 .
enet4-profile <profile-name>	Configures the duplex and speed of the Ethernet 4 interface on the AP. See ap enet-link-profile on page 241 .
event-thresholds-profile <profile-name>	Configures Received Signal Strength Indication (RSSI) metrics. See rf event-thresholds-profile on page 1245 .
exclude-mesh-cluster-profile-ap <profile-name>	Excludes the specified mesh cluster profile from this AP. The Secure Enterprise Mesh license must be installed.
exclude-virtual-ap <profile-name>	Excludes the specified virtual AP profiles from this AP.
exclude-wifi-uplink-profile <profile-name>	Excludes the specified Wi-Fi uplink profiles from this AP.
gps-service-profile <profile-name>	Configures GPS service profile.

Parameter	Description
ids-profile <profile-name>	Configures Aruba's IDS. See ids profile on page 706 .
iot <profile-name>	Applies iot related profile.
mesh-accesslist-profile	Configures the mesh access list profile.
mesh-cluster-profile <profile-name>	Configures the mesh cluster profile for the AP (mesh node). There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See ap mesh-cluster-profile on page 276 . The Secure Enterprise Mesh license must be installed.
priority <priority>	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The supported range of values is 1–16. The lower the number, the higher the priority. 1
mesh-radio-profile <profile-name>	Configures the 802.11g and 802.11a radio settings for the AP (mesh node). See ap mesh-ht-ssid-profile on page 279 . The Secure Enterprise Mesh license must be installed.
no	Negates any configured parameter.
regulatory-domain-profile <profile-name>	Configures the country code and valid channels. See ap regulatory-domain-profile on page 341 .
rf-optimization-profile <profile-name>	Configures load balancing and coverage hole and interference detection. See rf optimization-profile on page 1252 .
usb-profile <profile-name>	Configures USB profile.
virtual-ap <profile-name>	One or more profiles, each of which configures a specified WLAN. See wlan virtual-ap on page 4210 .

Parameter	Description
wifi-uplink-profile <profile-name>	Configures Wi-Fi uplink profile.
zigbee service-profile <profile-name>	Apply zigbee related profile.

Example

The following command excludes a virtual AP profile from a specific AP:

```
(host) [mynode] (config) #ap-name 00:0b:86:c0:cf:d8
(host) [mynode] (AP name "00:0b:86:c0:cf:d") #exclude-virtual-ap corpnet
```

Related Command

Command	Description
show ap-name	To view the AP settings.

Command History:

Release	Modification
ArubaOS 8.7.0.0	The following parameters were introduced: <ul style="list-style-type: none"> ■ airslice-profile ■ mesh-accesslist-profile
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap packet-capture

```
ap packet-capture
  clear <ap-name|ip-addr|ip6-addr>] <pcap-id> radio <0|1|2>
  close-port <port>
  interactive <ap-name|ip-addr|ip6-addr> <filter-spec> <target-ip> <target-port>
radio <0|1|2> channel <channel>
  open-port <port>
  pause <ap-name|ip-addr|ip6-addr> <pcap-id> radio <0|1|2>
  raw-start [<ap-name|ip-addr|ip6-addr>] <target-ip> <target-port> <format> radio
<0|1|2> channel <channel> maxlen <maxlen>
  resume [<ap-name|ip-addr|ip6-addr>] <pcap-id> radio <0|1|2>
  stop <ap-name|ip-addr|ip6-addr> <pcap-id> radio <0|1|2>
  wired-start <ap-name|ip-addr|ip6-addr> <target-ip> <target-port>
  wired-stop <ap-name|ip-addr|ip6-addr> <target-ip> <target-port>
```

Description

These commands manage WiFi packet capture (PCAP) on Aruba APs. The WiFi packets are encapsulated in a UDP header and sent to a client running a packet analyzer like Wildpacket's Airopeek, Omnipeek, or Wireshark.

These commands direct an AP to send Wi-Fi packet captures to a client packet analyzer utility such as Airmagnet, Wireshark and so on, on a remote client.

Before using these commands, you need to start the packet analyzer utility on the client and open a capture window for the port from which you are capturing packets. The packet analyzer cannot be used to control the flow or type of packets sent from APs.

The packet analyzer processes all packets. However, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the time stamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the AP.

Filter specification (used in ap packet-capture interactive) supports the following:

■ type (beacon/rts/cts/data/ack/ctrl/mgmt/all)

■ sta (mac address)

■ ssa (mac address)

■ sta (mac address)

■ ssa (mac address)

■ dir (tods, fromds)

■ retry (1, 0)

■ frag (1, 0)

■ wep (1, 0)

Filter spec examples:

(type eq beacon) or ((sta eq 000000010203) and (dir eq tods))

(type == data) && ((sta = 000000010203) || (sta == 000000010203))

(type != beacon)

(wep nq 1)

(type eq all)

Syntax

Parameter	Description
clear	Clears the packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
radio <0-2>	ID of the radio sending the packets
close-port <port>	(CPsec Campus APs and Remote APs only) Close or disallow access to this UDP port on the AP for packet capture purposes.
interactive	Start an interactive packet capture session between an AP and a client running a packet analyzer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<filter-spec>	Packet Capture filter specification. See Usage Guidelines for details.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.
radio <0-2>	ID of the radio sending the packets
channel <channel>	(Optional or Applicable only in AM mode) Number of a radio channel to tune into to capture packets.
open-port <port>	(CPsec Campus APs and Remote APs only) Enable or allow access to this UDP port on the AP for packet capture purposes.

Parameter	Description
pause	Pause a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
raw-start	Stream packets from the driver to a client running the packet analyzer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.
<format>	Packet capture format. Enter any number between 0 and 6 to select the one of the following formats: <ul style="list-style-type: none"> ▪ 0 - pcap ▪ 1 - peek ▪ 2 - airmagnet ▪ 3 - pcap+radio header ▪ 4 - ppi ▪ 5 - peek with 11n/11ac header ▪ 6 - radiotap
radio <0-2>	ID of the radio sending the packets
channel <channel>	(Optional or Applicable only in AM mode) Number of a radio channel to tune into to capture packets.
maxlen <maxlen>	(Optional) Limit the length of 802.11 frames to include in the capture to a specified maximum.
resume	Resume a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.

Parameter	Description
radio <0-2>	ID of the radio sending the packets.
stop	Stop a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
radio <0-2>	ID of the radio sending the packets
wired-start	Start a wired ethernet packet stream to an external viewer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.
wired-stop	Halt a wired ethernet packet stream currently being sent to an external viewer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.

Examples

The following command starts a raw packet capture session for the AP **ly115** on radio **0**, and sends the packets to the client at **10.64.102.4** on port **5000**.

```
(host) [mynode] (config) #ap packet-capture raw-start ap-name ly115
10.64.102.4 5000 0 radio 0
Packet capture has started for pcap-id:1
```

The following commands start an interactive packet capture session for the AP **ap1**.

```
#ap packet-capture open-port 5555
#ap packet-capture interactive ap-name ap1 "type eq all" 192.168.0.3 5555
radio 0
```

The output of the command in the example below displays packet capture session statistics for the AP **ap1**. In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, it will appear in a single, long table.

```
#show ap packet-capture status ap-name ap1

Packet Capture Sessions at ap1, IP 10.3.44.167
-----
pcap-id  filter      type      intf      channel max-pkts
-----  -
1        type eq all  interactive 6c:f3:7f:ba:65:70 153      0

max-pkt-size  num-pkts  status      url target      Radio ID
-----  -
65536        3759     in-progress 192.168.0.3/5555 0
```

Related Commands

Command	Description
vlan	To view the status of outstanding packet capture sessions.

Command History

Release	Modification
ArubaOS 8.6.0.0	Radio ID 2 was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Works in Access Point, AM, and Spectrum Monitor modes on all AP models in enable mode.

ap process restart

```
ap process restart  
  {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
```

Description

Use this command to restart the AP process of a particular AP. This command should only be used under the guidance of Aruba technical support.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IPv4 address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Conductor or managed devices.

ap provisioning-profile

```
ap provisioning-profile {default | <profile-name>}
  ap-lldp-pse-detect {disabled | enabled}
  ap-poe-power-optimization
  ap2xx-prestandard-poe-detection
  apdot1x-factory-cert
  apdot1x-passwd <apdot1x-passwd>
  apdot1x-timeout-bypass
  apdot1x-timeout-retries
  apdot1x-tls
  apdot1x-tls-suffix
  apdot1x-tls-suffix-domain <apdot1x-tls-suffix-domain>
  apdot1x-username <apdot1x-username>
  cellular_nw_preference {3g-only | 4g-only | advanced | auto}
  clone {default | <source>}
  link-priority-cellular <link-priority-cellular>
  link-priority-ethernet <link-priority-ethernet>
  link-priority-wifi <link-priority-wifi>
  master/conductor {clear | set <masterstr>/<conductorstr>}
  master-preference/conductor-preference <ipv4 | ipv6>
  no
  pppoe-passwd <pppoe-passwd>
  pppoe-service-name <pppoe-service-name>
  pppoe-user <pppoe-user>
  remote-ap
  uplink-vlan <uplink-vlan>
  usb-csr
  usb-dev <usb-dev>
  usb-dial <usb-dial>
  usb-init <usb-init>
  usb-modeswitch <usb-modeswitch [-v | -p | -V | -P | -M]>
  usb-passwd <usb-passwd>
  usb-power-mode {auto | enable | disable}
  usb-tty <usb-tty>
  usb-tty-control <usb-tty-control>
  usb-type
  usb-user <usb-user>
```

Description

This command defines a provisioning profile for an AP or group of APs. The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group by using the `ap-group <group> provisioning-profile <profile>` command.

In order to enable cellular uplink for a Remote AP it must have the device driver for the USB data card and the correct configuration parameters. ArubaOS includes device drivers for the most common hardware types, but you can use the `usb` commands in this profile to configure a Remote AP to recognize and use an unknown USB modem type.

Parameter	Description
<pre>ap provisioning-profile <profile-name></pre>	<p>Configures a provisioning profile for an AP or a group of APs. Give a name for the profile.</p>
<pre>ap-lldp-pse-detect</pre>	<p>Enabling causes the AP to detect the POE type via LLDP POE TLV. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ enabled: The AP uses PSE TYPE in the POE TLV to detect the PSE type. ■ disabled: The AP detects the POE using the HW classification.
<pre>ap-poe-power-optimization</pre>	<p>Enabling optimization minimizes the POE draw of the AP. Enabling optimization may disable some parts of the AP. Disabling optimization ensures all features are enabled. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ enabled: USB and Ethernet port (eth1) are shut down on AP. ■ disabled: AP operates in normal mode. <p>disabled</p>
<pre>ap2xx-prestandard-poe-detection</pre>	<p>Configures the prestandard PoE detection on 200 Series APs. The POE+ pre-standard detection is only available on 200 Series APs. It consists of a basic voltage comparator. If the line voltage is equal to or greater than 51 V, the PSE is assumed to be 802.3at compatible.</p>

Parameter	Description
<code>apdot1x-factory-cert</code>	Enables AP to use factory certificates when doing 802.1x EAP-TLS. Custom cert available.
<code>apdot1x-timeout-bypass</code>	Enables AP to be provisioned when 802.1X authentication times out.
<code>apdot1x-timeout-retries</code>	Sets the apdot1x timeout threshold. If the auth timeouts over this threshold, the AP will bypass apdot1x auth.
<code>apdot1x-passwd</code>	Sets the password of the AP to authenticate to 802.1X using PEAP.
<code>apdot1x-tls</code>	Enables AP to perform 802.1x authentication using EAP-TLS.
<code>apdot1x-tls-suffix</code>	Enables AP to use EAP-TLS username as suffix. disabled
<code>apdot1x-tls-suffix-domain <apdot1x-tls-suffix-domain></code>	Sets the suffix domain for AP dot1x EAP-TLS username. If defined, use EAP-TLS username as suffix, else use aruba.ap . 1-63
<code>apdot1x-username <apdot1x-username></code>	Sets the username of the AP to authenticate to 802.1X using PEAP.
<code>cellular_nw_preference</code> {3g-only 4g-only advanced auto}	The cellular network preference setting allows you to select how the modem should operate. <ul style="list-style-type: none"> ■ auto (default) ■ 3g_only: Locks the modem to operate only in 3G. ■ 4g_only: Locks the modem to operate only in 4G. ■ advanced: The

Parameter	Description
	<p>Remote AP controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach. Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.</p> <p>The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network.</p> <p>If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that</p>

Parameter	Description
	<p>alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.</p> <p>auto</p>
<p>clone <source></p>	<p>Clones an existing AP provisioning profile.</p>
<p>link-priority-cellular <link-priority-cellular></p>	<p>Sets the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.</p> <p>0-255 0</p>
<p>link-priority-ethernet <link-priority-ethernet></p>	<p>Sets the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.</p>
<p>link-priority-wifi <link-priority-wifi></p>	<p>Sets the priority of the wifi link.</p> <p>0-255</p>
<p>master/conductor</p>	<p>Changes the FQDN or IP address for the Mobility Conductor.</p>
<p>set <masterstr>/<conductorstr></p>	<p>Specifies the IP address or FQDN for the Mobility Conductor.</p>
<p>clear</p>	<p>Clear the definition for the Mobility Conductor in this profile.</p>

Parameter	Description
master preference/conductor preference <ipv4 ipv6>	Configures the preferred IP protocol (IPv4 or IPv6) for AP Conductor discovery. Default: IPv4
no	Negates any configured parameter.
pppoe-passwd <pppoe-passwd>	PPPoE password for the AP.
pppoe-servicename <pppoe-service-name>	PPPoE service name for the AP.
pppoe-user <pppoe-user>	PPPoE username for the AP.
remote-ap	Specifies that the profile is to be associated with a remote AP using certificates.
uplink-vlan <uplink-vlan>	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. If an AP is provisioned with an uplink VLAN, it must be connected to a trunk mode port or the frames of the AP will be dropped. 0-4095 0
usb-csr	Configures the USB storage for CSR and private Key file
usb-dev <usb-dev>	Configures the USB device identifier.

Parameter	Description
usb-dial <usb-dial>	Configures the dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
usb-init <usb-init>	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.
<pre>usb-modeswitch <usb-modeswitch> -v for default_vendor -p for default_product -V for target_vendor -P for target_product -M for message_content</pre>	<p>USB cellular devices on remote APs typically register as modems, but may occasionally register as a mass-storage device. If a remote AP cannot recognize its USB cellular modem, use the usb-modeswitch command to specify the parameters for the hardware model of the USB cellular data-card. You must enclose the entire modeswitch parameter string in quotation marks.</p>
usb-passwd <usb-passwd>	A PPP password, if provided by the cellular service provider.
<pre>usb-power-mode {auto enable disable}</pre>	Set the USB power mode to control the power to the USB port.
usb-tty <usb-tty>	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
<pre>usb-tty-control <usb-tty-control></pre>	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.
usb-type	<p>Specify the USB driver type.</p> <p>acm: Use ACM driver</p> <p>airprime: Use Airprime driver</p>

Parameter	Description
	<p>ether: Use CDC Ether driver for direct IP 4G device</p> <p>hso: Use HSO driver for newer Option</p> <p>huawei-cdc: Use Huawei driver for 4G device</p> <ul style="list-style-type: none"> ■ inetgear-gobi: Use Gobi driver for Netgear 340U or 341U 4G device ■ none: Disable 3G or 2G network on USB ■ option: Use Option driver ■ option-novatel-u620: Use Option driver for Novatel U620L 4G device ■ pantech-3g: Same as "pantech-uml290" - to support upgrade ■ pantech-auto: Use Pantech driver for Automatic modem mode ■ pantech-uml290: Use Pantech USB driver for UML290 device ■ ptumusbnet: Use Pantech USB driver for 4G device ■ rndis: Use a RNDIS driver for a 4G device ■ rndis-1800: Same as RNDIS - to use for L800 4G device ■ rndis-pantech-uml295: Use RNDIS driver for Pantech UML 295 4G device ■ sierra-evdo: Use EVDO Sierra Wireless driver ■ sierra-gsm: Use GSM Sierra Wireless driver ■ sierrausbnet: Use SIERRA Direct IP driver for 4G device ■ storage: Use USB flash as storage device for storing Remote AP certificates

Parameter	Description
usb-user <usb-user>	The PPP username provided by the cellular service provider.

Examples

The following commands create a provisioning profile named `profile_branch`, in which the cellular link is the primary uplink because it has a higher priority than the Ethernet link:

```
(host) [mynode] (config) #ap provision-profile profile_branch
(host) [mynode] (Provisioning profile "profile_branch") #link-priority-cellular 2
(host) [mynode] (Provisioning profile "profile_branch") #link-priority-ethernet 1
(host) [mynode] (Provisioning profile "profile_branch") #usb-type acm
(host) [mynode] (Provisioning profile "profile_branch") #usb-modeswitch "-v 0x106c -p 0x3b06 -V 0x106c -P 0x3717 -M 5534243b82e238c24000000800008ff0200000000000000000000000000000000"
```

The following example configures the preferred IP protocol for AP master/conductor discovery:

```
(host) [mynode] (config) #ap provision-profile profile_branch
(host) [mynode] (Provisioning profile "profile_branch") #master/conductor-preference ipv6
```

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following parameters have been modified: All instances of <code>master</code> have been replaced with <code>conductor</code> . All instance of <code>master-preference</code> have been replaced with <code>conductor-preference</code> .

Release	Modification
	All instance of <code>masterstr</code> have been replaced with <code>conductorstr</code> .
ArubaOS 8.8.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>apdot1x-timeout-bypass</code> ■ <code>apdot1x-timeout-retries</code>
ArubaOS 8.7.0.0	The <code>master-preference</code> parameter was introduced.
ArubaOS 8.4.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>apdot1x-tls-suffix</code> ■ <code>apdot1x-tls-suffix-domain</code>
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>apdot1x-factory-cert</code> ■ <code>apdot1x-tls</code> ■ <code>ap-lldp-pse-detect</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap provisioning-rule

```
ap provisioning-rule <profile-name>
  action
    a-ant-gain <a-ant-gain>
    ap-group <ap-group>
    g-ant-gain <g-ant-gain>
    radio-0-5ghz-ant-gain <radio-0-5ghz-ant-gain>
    radio-1-5ghz-ant-gain <radio-1-5ghz-ant-gain>
  clone <source>
  condition
    any-ap
    ap-type <ap-model>
    ip-range {<start> <end>}
    network {<ipaddr> <mask_len>}
  no...
```

Description

This command defines the conditions to select a group of APs and the subsequent actions to provision the APs. These settings can be saved or assigned to an AP group via the command `ap provisioning-rule <profile-name>`.

Parameter	Description
<code>ap provisioning-rule <profile-name></code>	Configures a condition for a group of APs and the related actions to provision the APs. Give a name for the profile.
<code>action</code>	Specify action that corresponds to the conditions, when rule is applied. When an AP satisfies all the criteria in conditions, the managed device executes the actions.
<code>a-ant-gain <a-ant-gain></code>	Antenna gain for 802.11a (5 GHz) antenna.
<code>ap-group <ap-group></code>	Name of the AP group to which the AP belongs.
<code>g-ant-gain <g-ant-gain></code>	Antenna gain for 802.11g (2.4 GHz) antenna.
<code>radio-0-5ghz-ant-gain <radio-0-5ghz-ant-gain></code>	Antenna gain for radio 0 (5 GHz) antenna. This parameter is only needed for APs that support dual 5 GHz mode.

Parameter	Description
<code>radio-1-5ghz-ant-gain <radio-1-5ghz-ant-gain></code>	Antenna gain for radio 1 (5 GHz) antenna. This parameter is only needed for APs that support dual 5 GHz mode.
<code>clone <source></code>	Copy data from another AP provisioning rule.
<code>condition</code>	Specify conditions to narrow the scale of AP based on each criteria in the conditions.
<code>any-ap</code>	Specify this provisioning rule's condition to any AP. The rule with this condition has lowest priority and is applied only when other conditions are not met.
<code>ap-type <ap-type></code>	Specify specific AP models that match with unprovisioned APs.
<code>ip-range {<start> <end>}</code>	Apply the AP provisioning rules to the specified IPv4/IPv6 address range. It contains the following parameters: <ul style="list-style-type: none"> ■ <code>start</code>: Starting IPv4/IPv6 address of the range. ■ <code>end</code>: Ending IPv4/IPv6 address of the range.
<code>network {<ipaddr> <mask_len>}</code>	Specify network that matches with unprovisioned APs in this subnet. It has the following parameters: <ul style="list-style-type: none"> ■ <code>addr</code>: IPv4/IPv6 address. ■ <code>mask_len</code>: Prefix/length of the netmask.
<code>no</code>	Remove any existing configuration.

Examples

The following commands add the condition and associated action for an auto-provisioning profile:

```
(host) [mm] (config) #ap provisioning-rule test
(host) [mm] (ap provisioning rule "test") #condition ap-type AP-103
(host) [mm] (ap provisioning rule "test") #action ap-group corp1
```

Related Commands

Command	Description
show ap provisioning-rule	This command displays the details of an AP auto-provisioning rule.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap provisioning-rules

```
ap provisioning-rules <profile-name>  
no...  
provision-rule [<rule> {priority <priority>}]
```

Description

This command defines the priority of the provisioning rules that are actively used by the Auto-provisioning feature in APs.

Parameter	Description
no	Removes any existing configuration.
provision-rule <rule>	Specify action that corresponds to the conditions, when a rule is applied. When an AP satisfies all the criteria in conditions, the managed device executes the actions.
priority <priority>	Specify the priority level to determine the precedence of the rules. The lowest value takes highest priority. 1-64

Example

The following command defines the priority of the rule for an auto-provisioning profile:

```
(host) [mm] (ap provisioning rules) #provision-rule rule1 priority 1
```

Related Commands

Command	Description
show ap provisioning-rules	This command displays information about the priority level of AP provisioning rules.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap randomize-channel

```
ap randomize channel ap-group <ap-group> phy-type <phy-type>
```

Description

This command will instruct the AP to change to a random channel and this command works only when ARM is in maintain mode.

Parameter	Description
ap-group <ap-group>	Name of the AP group.
phy-type <phy-type>	PHY Type of Radio. Possible values are '80211a' and '80211g'

Example

The following command instruct the AP to change to a random channel:

```
(host) [mynode] ap randomize-channel ap-group default phy-type 80211a
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap redeploy controller-less

```
ap redeploy controller-less
  all
  ap-group <ap-group>
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  wired-mac <wired-mac>
```

Description

This command sets the AP preference role to controller-less, allowing the AP to bypass controller discovery and immediately initiate Instant discovery during AP image upgrade. APs with the controller-less preference role are deployed as controller-less APs.



The `ap redeploy controller-less` command is applicable to Unified APs (UAPs) only.

Parameter	Description
<code>all</code>	Deploys all APs as controller-less APs.
<code>ap-group <ap-group></code>	Deploys all APs in the specified AP group as controller-less APs.
<code>ap-name <ap-name></code>	Deploys a specific AP as a controller-less AP.
<code>ip-addr <ip-addr></code>	Deploys the AP with a specific IP address as a controller-less AP.
<code>ip6-addr <ip6-addr></code>	Deploys the AP with a specific IPv6 address as a controller-less AP.
<code>wired-mac <wired-mac></code>	Deploys the AP with a specific MAC address as a controller-less AP.

Example

The following command deploys all APs as controller-less APs.

```
(host) [mynode] #ap redeploy controller-less all
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap-regroup

```
ap-regroup {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <group>
```

Description

This command moves a specified AP into a group. All APs discovered by the Mobility Conductor are assigned to the “default” AP group. An AP can belong to only one AP group at a time. You can move an AP to an AP group that you created with the `ap-group` command.



This command automatically reboots the AP.

Parameter	Description
ap-name	Name of the AP.
serial-num	Serial number of the AP.
wired-mac	MAC address of the AP.
<group>	Name that identifies the AP group. The name must be 1-63 characters.

Example

The following command moves an AP to the ‘corpnet’ group:

```
(host) [mynode] (config) #ap-regroup wired-mac 00:0f:1e:11:00:00 corpnet
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

ap regulatory activate

ap regulatory activate <filename>

Description

This command activates the specified regulatory certificate

Parameter	Description
<filename>	Name of the regulatory certificate to be activated.

Related Commands

Command	Description
show ap regulatory	This command displays information about the current regulatory certificate.
show ap allowed-channels	This command displays information about the supported channels.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap regulatory-domain-profile

```
ap regulatory-domain-profile {default | <profile-name>
  clone <source>}
  country-code <country-code>
  no
  oob_switch
  utb_filter_block <5GHz | 6GHz>
  valid-11a-160mhz-channel-group <valid-11a-160mhz-channel-group>
  valid-11a-40mhz-channel-pair <valid-11a-40mhz-channel-pair>
  valid-11a-80mhz-channel-group <valid-11a-80mhz-channel-group>
  valid-11a-channel <valid-11a-channel>
  valid-11g-40mhz-channel-pair <valid-11g-40mhz-channel-pair>
  valid-11g-channel <valid-11g-channel>
  valid-6ghz-channel <valid-6ghz-channel>
```

Description

This command configures an AP regulatory domain profile. This profile configures the country code and valid channels for operation of APs. The list of valid channels only affects the channels that may be selected by ARM or by the Mobility Conductor when no channel is configured. Channels that are specifically configured in the AP radio settings profile (see [rf dot11a-radio-profile](#), [rf dot11g-radio-profile](#), [rf dot11g-radio-profile](#)) must be valid for the country and the AP model.

A Mobility Conductor shipped to certain countries, such as the U.S. and Israel, cannot terminate APs with regulatory domain profiles that specify different country codes from the Mobility Conductor. For example, if a controller is designated for the U.S., then only a regulatory domain profile with the “US” country code is valid; setting APs to a regulatory domain profile with a different country code will result in the radios not coming up. For controllers in other countries, you can mix regulatory domain profiles on the same controller; for example, one controller can support APs in Japan, Taiwan, China, and Singapore.

In order for an AP to boot correctly, the country code configured in the AP regulatory domain profile must match the country code of the LMS. If none of the channels supported by the AP have received regulatory approval by the country whose country code you selected, the AP will revert to Air Monitor mode.

This command is used to override available channels in the list of channels allowed for use in that country. If you do not add any channels to the AP regulatory domain profile, it means the AP can use any of the available channels. If you want to disable use of an entire band, best practices is to use the `rf-dot11a-radio-profile`, `rf-dot11g-radio-profile`, Or `rf dot11-6ghz-radio-profile` commands to disable the radio. Alternatively, if you want to disable a specific bandwidth, use the **Max Channel Bandwidth** and **Min Channel Bandwidth** settings in the radio profiles, and AirMatch will enforce this setting.



After an upgrade, the 6 GHz channel information is not populated in the existing regulatory domain profile by default. To add 6 GHz channels, you must change the country code to a different country code, apply the change, and then revert it to the original country code. Another option is to create a new profile or copy the existing regulatory domain profile into a new regulatory domain profile to save the configuration.

Parameter	Description
<code>ap regulatory-domain-profile <profile></code>	Configures a Regulatory Domain profile. Give a name to this instance of the profile. The name must be 1-63 characters long.
<code>clone <source></code>	Name of an existing regulatory domain profile from which parameter values are copied.
<code>country-code <country-code></code>	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.
<code>no</code>	Negates any configured parameter.
<code>oob_switch</code>	If enabled, OOB scanning on 6 GHz band is allowed. If disabled OOB scanning on 6 GHz band is blocked. This switch is valid only for AP-615 access points in the 5GHz-and-2.4GHz operation mode. Disable the switch to enable the use of UNII-4 band. Default: Enabled.
<code>utb_filter_block</code>	This parameter is used to control the band on which the UTB limitation is applied in the regulatory-domain-profile. The utb filter supports channel band on both 5 GHz and 6 GHz. Listed below are the two options available: <ul style="list-style-type: none">▪ 5 GHz - Select 5 GHz for upper band blocking.▪ 6 GHz - Select 6 GHz for lower band blocking. Default value: 6 GHz

Parameter	Description
<code>valid-11a-40mhz-channel-pair</code> <code><valid-11a-40mhz-channel-pair></code>	<p>Specifies a channel pair valid for 40 MHz operation in the 802.11a frequency band for the specified regulatory domain. The two channels must be separated by a dash. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-11a-80mhz-channel-group</code> <code><valid-11a-80mhz-channel-group></code>	<p>Specifies which 80 MHz channels on the <i>a</i> band are available for assignment by ARM and for Mobility Conductor to randomly assign if the user has not specified a channel. The channel numbers below correspond to channel center frequency. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-11a-160mhz-channel-group</code> <code><valid-11a-160mhz-channel-group></code>	<p>Specifies a valid 802.11a channel group for 160 MHz channel on the <i>a</i> band. The channel numbers below correspond to channel center frequency. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-11a-channel</code> <code><valid-11a-channel></code>	<p>Specifies a single 802.11a channel number for 20 MHz operation within the specified regulatory domain. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-11g-40mhz-channel-pair</code> <code><valid-11g-40mhz-channel-pair></code>	<p>Specifies a channel pair valid for 40 MHz operation in the 802.11g frequency band for the specified regulatory domain. The two channels must be separated by a dash. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-11g-channel</code> <code><valid-11g-channel></code>	<p>Specifies a single 802.11g channel number for 20 MHz operation within the specified regulatory domain. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>
<code>valid-6ghz-channel</code> <code><valid-6ghz-channel></code>	<p>Specifies a single 6 GHz channel number within the specified regulatory domain. Changing the country code causes the valid channel lists to be reset to the defaults for the country.</p>

Examples

The following example configures the regulatory domain profile for APs in Japan:

```
(host) [mynode] (config) #ap regulatory-domain-profile rd1
(host) [mynode] (Regulatory Domain profile "rd1") #country-code JP
```

The following example configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 36 and 40, is allowed for 40 MHz mode of operation on the 5 GHz frequency band:

```
(host) [mynode] (config) #ap regulatory-domain-profile usa1
(host) [mynode] (Regulatory Domain profile "usa1") #country-code US
(host) [mynode] (Regulatory Domain profile "usa1") #valid-11a-40mhz-channel-pair 36-40
```

The following example configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 5 and 1, is allowed for 40 MHz mode of operation on the 2.4 GHz frequency band:

```
host) [mynode] (config) #ap regulatory-domain-profile usa1
host) [mynode] (Regulatory Domain profile "usa1") #country-code US
host) [mynode] (Regulatory Domain profile "usa1") #valid-11g-40mhz-channel-pair 1-5
```

The following example configures a regulatory domain profile for a Wi-Fi 6E AP specifying the country code and 6 GHz channel on the 6 GHz radio band (ArubaOS 8.9.0.0 or later versions).

```
host) [mynode] (config) #ap regulatory-domain-profile reg-635
host) [mynode] (Regulatory Domain profile "reg-635") #country-code US
host) [mynode] (Regulatory Domain profile "reg-635") #valid-6ghz-channel 165
```

The following example configures a UTB Filter Blocking parameter for 5 GHz band (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #ap regulatory-domain-profile reg-635
(host) [mynode] (Regulatory Domain profile "reg-635") #utb_filter_block
(host) [mynode] (Regulatory Domain profile "reg-635") #utb_filter_block 5GHz
```

The following example configures AP's regulatory domain profile:

```
(host) [/md] (config) #ap regulatory-domain-profile
clone                Copy data from another Regulatory Domain profile
country-code         Country Code
```

```

no                Delete Command
oob_switch        enabled - allows OOB scanning on 6GHz Band. disabled
- blocks OOB scanning on 6GHz Band. Default enabled.
utb_filter_block  6GHz - Selects 6GHz lowerband blocking. 5GHz -
Selects 5GHz upper band blocking. Default 6GHz.
valid-11a-160mhz-chan.. Valid 802.11a channel group for 160MHz (e.g., 36-64)
valid-11a-40mhz-chann.. Valid 802.11a channel pair for 40MHz (e.g., 36-40)
valid-11a-80mhz-chann.. Valid 802.11a channel group for 80MHz (e.g., 36-48)
valid-11a-channel  Valid 802.11a channel
valid-11g-40mhz-chann.. Valid 802.11g channel pair for 40MHz (e.g., 1-5)
valid-11g-channel  Valid 802.11g channel
valid-6ghz-channel Valid 6GHz channel

```

Related Commands

Command	Description
show ap allowed-channels	To view the supported channels.

Command History

Release	Modification
ArubaOS 8.11.0.0	The oob_switch parameter was introduced.
ArubaOS 8.9.0.0	The following parameters were introduced: <ul style="list-style-type: none"> utb_filter_block (RT-6923-Rashmi) valid-6ghz-channel <valid-6ghz-channel>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap regulatory reset

ap regulatory reset

Description

This command returns the Mobility Conductor to the factory default Regulatory-Cert.

Related Commands

Command	Description
show ap regulatory	This command displays information about the current regulatory certificate.
show ap allowed-channels	This command displays information about the supported channels.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap remote-debug-pkt

```
ap remote-debug-pkt [dump [start|stop]|match|mirror|reset|type] [ap-name <ap-name>|ip-addr<ip-addr>|ip6-addr<ip6-addr>]
```

Description

This command enables the packet debugging functionality to debug and troubleshoot data packets handled by the AP. Configure the packet debugging functionality by issuing the **ap remote-debug-pkt type** and **ap remote-debug-pkt match** to select the packet data type and filter respectively.



The **ap remote-debug-pkt type** command is necessary to select the debugging type, whereas **ap remote-debug-pkt match** is an optional command. If no match is configured, the filter is not applied and all the data packets are logged.

Issue the **ap remote-debug-pkt dump** command to view the selected data packets and **ap remote-debug-pkt mirror ip-addr <ip-addr>** command to mirror the data packets to a network device. The **ap remote-debug-pkt reset** command clears the packet debugging configuration.

Parameter	Description
<code>dump [start stop]</code>	Start or stop the debug packet dump to display data packets of the selected type .
<code>match [ap-name <ap-name> ip-addr<ip-addr> ip6-addr<ip6-addr>]</code>	Filter packets based on the AP name, IPv4 address, or IPv6 address.
<code>mirror [ap-name <ap-name> ip-addr<ip-addr> ip6-addr<ip6-addr>]</code>	Mirror the specified packets to the network device at the mentioned IPv4 or IPv6 address.
<code>reset [ap-name <ap-name> ip-addr<ip-addr> ip6-addr<ip6-addr>]</code>	Reset the packet debugging configuration.
<code>type [ap-name <ap-name> ip-addr<ip-addr> ip6-addr<ip6-addr>]</code>	Select the packet type for debugging. Debugging packet types include the following packet types: arp , dhcp , and all .

Example

The following command starts and stops the debug packet dump for specified AP name.

```
(host) [mynode] #ap remote-debug-pkt dump <start/stop> ap-name <ap-name>
```

Related Command

Command	Description
show ap remote-debug-pkt	Issue this command to display the packet debugging details of an AP.

Command History

Release	Modification
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap-rename

```
ap-rename {ap-name <name>|serial-num <num>|wired-mac <macaddr>} >
```

Description

This command changes the name of an AP to the specified new name. An AP name must be unique within your network.



This command automatically reboots the AP.

Parameter	Description
ap-name	Current name of the AP.
serial-num	Serial number of the AP.
wired-mac	MAC address of the AP.

Example

The following command renames an AP:

```
(host) [mynode] (config) #ap-rename wired-mac 00:0f:1e:11:00:00 building3-lobby
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

ap sesimagotag-esl ugr-radio-firmware

```
ap sesimagotag-esl ugr-radio-firmware tftp <tftphost> <filename> all <global|local>
| ap-group <ap-group> | ap-name <ap-name> | ip-addr <ip-addr> | wired-mac <wired-
mac>
```

Description

This command will upgrade the ESL-Radio Firmware.

Parameter	Description
tftp <tftphost>	IPv4 address of the TFTP server
<filename>	File name of the TFTP server.
all	Upgrades ESL-Rado Firmare of all Aps.
global	Upgrades APs on all controllers.
local	Upgrades APs on the present controllers
ap-group <ap-group>	Name of the AP group.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
wired-mac	MAC address of the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap spectrum clear-webui-view-settings

ap spectrum clear-webui-view-settings

Description

Clear a saved spectrum dashboard view. Saved spectrum view preferences may not be backwards compatible with the spectrum analysis dashboard in earlier versions of ArubaOS. If you downgrade to an earlier version of ArubaOS and your client is unable to load a saved spectrum view in the spectrum dashboard, access the CLI in enable mode and issue this command to delete the saved spectrum views and display default view settings in the spectrum dashboard.

Example

The following command removes the WebUI spectrum view settings file of an user:

```
(host) [mynode] #ap spectrum clear-webui-view-settings
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license.	Enable mode on Mobility Conductor.

ap spectrum local-override

```
no  
override ap-name <ap-name> spectrum-band <2.4ghz | 5ghz>
```

Description

Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list. There are two ways to change an AP that supports the spectrum monitor feature into a spectrum monitor. You can assign that AP to a 802.11a and 802.11g radio profile that is already set to spectrum mode, or you can temporarily change the AP into a spectrum monitor using a local spectrum override profile. When you use a local spectrum override profile to override the mode setting of an AP, that AP will begin to operate as a spectrum monitor, but will remain associated with its previous 802.11a and 802.11g radio profiles. If you change any parameter (other than the overridden mode parameter) in the spectrum monitor's 802.11a or 802.11g radio profiles, the spectrum monitor will immediately update with the change. When you remove the local spectrum override, the spectrum monitor will revert back to its previous mode, and remain assigned to the same 802.11a and 802.11g radio profiles as before.

Parameter	Description
no	Negates any previous AP spectrum local-override configuration
override ap-name <ap-name>	Specifies the name of an AP whose radio should be converted to a spectrum monitor radio.
spectrum band	Specifies the spectrum band or portion of the band to be monitored by the spectrum monitor radio For 2GHz, channels 1–14 For 5 GHz, channels 36–64, 100–140 and 149–165 2 GHz

Related Commands

Command	Description
show ap spectrum local-override	This command shows a list of AP radios currently converted to spectrum monitors via the spectrum local-override list.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license.	Config mode on Mobility Conductor.

ap system-profile

```
ap system-profile <profile-name>
  aeroscout-rtls-server ip-or-dns <ipaddr-or-dns> port <port> include-unassoc-sta
  {disable|enable}
  airmatch-measure-duration <airmatch-measure-duration>
  airmatch-report-enabled
  airmatch-report-period <airmatch-report-period>
  am-scan-rf-band {a | all | g}
  ap-arp-attack-protection
  ap-console-password <ap-console-password>
  ap-console-protection
  ap-deploy-hour
  ap-poe-mode {failover | shared}
  ap-usb-power-mode {auto | enable | disable}
  bkup-band {a | all | g}
  bkup-lms-ip <ipaddr>
  bkup-lms-ipv6 <ipaddr>
  bkup-mode {static | dynamic | off}
  bkup-passwords <password>
  ble-op-mode {Beaconing | Disabled | DynamicConsole | PersistentConsole}
  bootstrap-threshold <number>
  bridge-offload
  clone {default | <source>}
  console-enable
  console-log-lvl
  disable-factory-reset
  disable-tftp-image-upgrade
  dns-domain <domain>
  double-encrypt
  driver-log-level <severity-level>
  dscp-to-dot1p-priority-mapping <dscp-to-dot1p-priority-mapping>
  dual-5ghz-mode {automatic | disabled | enabled}
  dump-server <dump-server>
  dump-collection-profile {default | profile-name}
  flex-radio-mode {2.4GHz|2.4GHz-and-5GHz|5GHz}
  flex-dual {2.4GHz-and-6GHz|5GHz-and-2.4GHz|5GHz-and-6GHz}
  flex-dual-mode {2.4GHz-and-6GHz|5GHz-and-2.4GHz|5GHz-and-6GHz|Automatic}
  gre-offload
  he-pooling-enable
  health-check [burst size <burst-size> | frequency <frequency> | mode <mode> |
  packet-size <packet-size>| report <report>| retries <retries>}
  health-check-option
  heartbeat-dscp <heartbeat-dscp>
  heartbeat-interval <heartbeat-interval>
  image-url <image-url>
  ipm-enable
  ipm-power-reduction-step-prio {all | ipm-step {cpu_throttle_25 | cpu_throttle_50
  | cpu_throttle_75 | disable_alt_eth | disable_pse | disable_usb | radio_2ghz_
  chain_1x1 | radio_2ghz_chain_2x2 | radio_2ghz_chain_3x3 | radio_2ghz_power_3dB |
  radio_2ghz_power_6dB | radio_2ghz_disable | radio_5ghz_chain_1x1 | radio_5ghz_
  chain_2x2 | radio_5ghz_chain_3x3 | radio_5ghz_power_3dB | radio_5ghz_power_6dB |
  radio_5ghz_disable | radio_5ghz_2_chain_1x1 | radio_5ghz_2_chain_2x2 | radio_
  5ghz_2_chain_3x3 | radio_5ghz_2_power_3dB | radio_5ghz_2_power_6dB | radio_5ghz_
```

```

2_disable | radio_6ghz_chain_1x1 | radio_6ghz_chain_2x2 | radio_6ghz_chain_3x3 |
radio_6ghz_disable | radio_6ghz_power_3dB | radio_6ghz_power_6dB } priority
<priority>}
(For versions prior to ArubaOS 8.11.0.0)
ipm-power-reduction-step-prio {all | ipm-step {cpu_throttle_25 | cpu_throttle_50
| cpu_throttle_75 | disable_alt_eth | disable_pse1 | disable_pse2 | disable_usb |
radio_1_chain_1x1 | radio_1_chain_2x2 | radio_1_chain_3x3 | radio_1_power_3dB |
radio_1_power_6dB | radio_1_disable | radio_0_chain_1x1 | radio_0_chain_2x2 |
radio_0_chain_3x3 | radio_0_chain_4x4 | radio_0_chain_5x5 | radio_0_chain_6x6 |
radio_0_chain_7x7 | radio_0_power_3dB | radio_0_power_6dB | radio_0_disable |
radio_2_chain_1x1 | radio_2_chain_2x2 | radio_2_chain_3x3 | radio_2_power_3dB |
radio_2_power_6dB | radio_2_disable | radio_2_chain_1x1 | radio_2_chain_2x2 |
radio_2_chain_3x3 | radio_2_disable | radio_2_power_3dB | radio_2_power_6dB }
priority <priority>} (ArubaOS 8.11.0.0 or later versions)
itm-enable
led-mode {normal | off}
led-override
lms-hold-down-period <lms-hold-down-period>
lms-ip <lms-ip>
lms-ipv6 <lms-ipv6>
lms-ping-interval <lms-ping-interval>
lms-preemption
maintenance-mode
max-request-retries <max-request-retries>
mcast-aggr
mcast-aggr-allowed-vlan <vlan-list>
mgmt-dscp <mgmt-dscp>
mtu <mtu>
native-vlan-id <native-vlan-id>
no
number_ipsec_retries <number_ipsec_retries>
pmm-report-min-interval
rap-bw-resv-1 acl <aclname> <bw-value> [priority <priority>]
rap-bw-resv-2 acl <acl-name> <bw-value> [priority <priority>]
rap-bw-resv-3 acl <acl-name> <bw-value> [priority <priority>]
rap-bw-total <rap-bw-total>
rap-corp-dns-server <ipv4 address>
rap-corp-dns-server_ipv6 <ipv6 address>
rap-dhcp-default-router <rap-dhcp-default-router>
rap-dhcp-dns-server <rap-dhcp-dns-server>
rap-dhcp-lease <rap-dhcp-lease>
rap-dhcp-pool-end <rap-dhcp-pool-end>
rap-dhcp-pool-netmask <rap-dhcp-pool-netmask>
rap-dhcp-pool-start <rap-dhcp-pool-start>
rap-dhcp-server-id <rap-dhcp-server-id>
rap-dhcp-server-vlan <rap-dhcp-server-vlan>
rap-gre-mtu <rap-gre-mtu>
rap-local-network-access
recovery-mode {auto | legacy}
request-retry-interval <request-retry-interval>
rf-band <a | g>
rtls-server ip-or-dns <ip-or-dns> port <port> key <key> station-message-frequency
<seconds> [include-unassoc-sta {enable | disable}]
rtls-server-compat_mode
secondary-master/secondary-conductor <secondary-master>/<secondary-conductor>
sesImagotag-esl-channel

```

```

sesImagotag-esl-radio-coexistence
sesImagotag-esl-server
sesImagotag-esl-serverip
sesImagotag-esl-tls-auth
sesImagotag-esl-tls-fqdn-verify
session-acl <session-acl>
slow_timer_recovery
spanning-tree
split-5ghz-mode
syscontact <syscontact>
telnet
wids-ampdu-optimization
wired-poe-bounce-interval <wired-poe-bounce-interval>
wired-port-bounce-interval <wired-port-bounce-interval>

```

Description

This command configures an AP system profile. The AP system profile configures AP administrative operations, such as AirMatch and AP health check options and logging levels.

By default, each AP in a Mobility Conductor deployment measures its RF environment for a 5-minute duration, every 30 minutes. The Mobility Conductor uses this information to compute an optimal solution, then deploys the latest RF plan by sending updated settings to the APs. Use the **airmatch** settings in the AP system profile to modify these default report intervals, or to disable or re-enable AirMatch reports to the APs.

The AP Health check feature configured via the `health-check` parameters uses ping probes to check reachability and latency levels for the connection between the AP and the managed devices. Recorded latency information appears in the output of the `show ap ip health-check` command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (`tmp` or `ap_hcm_log`) on the AP.

Starting from ArubaOS 8.2.0.0, the `no ipm-power-reduction-step-prio ipm-step <ipm-step> priority <priority number> sub-command` for the `ap system-profile <profile>` command set is simplified. If you want to remove one step or priority, you only need to specify the step and not the priority. For example: `no ipm-power-reduction-step-prio ipm-step <ipm-step>`.

Parameter	Description
<code>ap system-profile <profile></code>	Configures AP system profile. Give a name for this instance of the profile. The name must be 1-63 characters long.
<code>aeroscout-rtls-server</code>	Enables the AP to send RFID tag information to an AeroScout RTLS server.

Parameter	Description
	RTLS station reporting includes information for APs and the clients that the AP has detected.
ip-or-dns <ip-or-dns>	IPv4/IPv6 address or the DNS of the AeroScout server to which location reports are sent.
port <port>	Port number on the AeroScout server to which location reports are sent.
include-unassoc-sta enable disable	If you select the include-unassoc-sta enable option, the station reports will also include information about clients not associated to any AP. By default, unassociated clients are not included in station reports. disabled
airmatch-measure-duration <airmatch-measure-duration>	Change the AirMatch RF measurement duration from the default value of 5 minutes to any value in the range 5–60 minutes. A value of 0 disables AirMatch RF environment measurements. 5-60 5

Parameter	Description
airmatch-report-enabled	<p>Each AP in a Mobility Conductor deployment measures its RF environment for a duration specified by airmatch-measure-duration, every 30 minutes by default. Mobility Conductor uses this information to compute an optimal solution.</p> <p>enabled</p>
airmatch-report-period <airmatch-report-period>	<p>Change the frequency period which AirMatch starts measuring the RF environment.</p> <p>5-180 minutes.</p> <p>30</p>
am-scan-rf-band	<p>Scanning band for multiple RF radios.</p> <p>a, g, all</p> <p>all</p>
a	Sets the scanning band to 802.11a only.
g	Sets the scanning band to 802.11g only.
all	Sets the scanning band to apply to all bands.
ap-arp-attack-protection	<p>Drop ARP packets coming from wired or wireless clients with AP gateway IP address. In other words, disallow ARP attack from untrusted ports.</p> <p>enabled</p>

Parameter	Description
<pre>ap-console-password <ap-console-password></pre>	<p>Set the AP console password on the managed device. If the user does not set any password, the managed device generates a default random password which can be viewed by executing the encrypt disable command followed by the show ap system-profile <profile-name> command.</p> <p>6-32</p>
<pre>ap-console-protection</pre>	<p>Enable the AP console password.</p> <p>enabled</p>
<pre>ap-deploy-hour</pre>	<p>Configure hour-of-day for solution deployment for all radios of an AP. Overrides Airmatch profile if a valid hour is specified.</p> <p>0-23</p>
<pre>ap-poe-mode {failover shared}</pre>	<p>Configure the required PoE mode on the AP platforms that support dual PoE mode.</p> <ul style="list-style-type: none"> ■ Failover: Enables the source PoE power from either of the Ethernet ports. ■ Shared: Enables the combined power from both the PoE sources.
<pre>ap-usb-power-mode {auto enable disable}</pre>	<p>Set the USB power mode to control the power to the USB port. Listed below are the power modes:</p> <ul style="list-style-type: none"> ■ auto- Detect USB power mode automatically

Parameter	Description
	<ul style="list-style-type: none"> ■ disable- Disable USB power ■ enable- Enable USB power <p>This parameter can be configured only on AP-214, AP-215, AP-224, AP-225, AP-205H, AP-303H, AP-304, AP-305, AP-314, AP-315, AP-324, AP-325, AP-334, AP-335, AP-344, AP-345, AP-203R, and AP-203RP access points only.</p> <p>auto</p>
<pre>bkup-band a all g</pre>	<p>Band on which the Mobility Conductor broadcasts the backup ESSID.</p> <p>a, g, all</p> <p>all</p>
<pre>bkup-lms-ip <bkup-lms-ip></pre>	<p>In multi-controller) networks, specifies the IP address of a <i>backup</i> to the IP address specified with the <i>lms-ip</i> parameter.</p>
<pre>bkup-lms-ipv6 <bkup-lms-ipv6></pre>	<p>In multi-controller IPv6 networks, specifies the IPv6 address of a <i>backup</i> to the IPv6 address specified with the <i>lms-ipv6</i> parameter.</p>

Parameter	Description
<pre>bkup-mode dynamic off static</pre>	<p>This parameter allows AP console access using a backup ESSID, allowing users to access an AP console after the AP has disconnected from the Mobility Conductor. When the AP advertises a backup ESSID in either static or dynamic mode, a user is able to access and debug the AP remotely through a virtual AP. Select dynamic or static to enable this feature and select the mode by which the Mobility Conductor broadcasts the backup ESSID. This feature is disabled by default.</p> <p>dynamic, off, static off</p>
<pre>bkup-passwords <bkup-passwords></pre>	<p>Allows client access to adjust the band and mode settings for the backup ESSID.</p>
<pre>ble-op-mode {Beaconing Disabled DynamicConsole PersistentConsole}</pre>	<p>Determines how the built-in BLE chip in the AP functions. BLE chip can be in one of the following four modes:</p> <ul style="list-style-type: none"> ■ Beaconing: The built-in BLE chip of the AP functions as an iBeacon combined with beacon management functionality. ■ Disabled: The built-in BLE chip of the AP is turned off. This is the default setting. ■ DynamicConsole: The built-in chip of

Parameter	Description
	<p>the AP functions as a regular iBeacon combined with beacon management functionality. However, when the link to the Mobility Conductor is lost, the built-in chip temporarily enables access to the AP console over BLE. This state of the BLE device may be rolled back to any of the other modes if the AP receives a different configuration setting for the ble-op-mode parameter from the new LMS.</p> <ul style="list-style-type: none"> <p>PersistentConsole : The built-in chip of the AP provides access to the AP console over BLE using a mobile application. This functionality is the superset of the Beaconing mode.</p> <p>BLE is disabled on ArubaOS FIPS build.</p> <p>disabled</p>
ble-token <ble-token>	<p>The BLE endpoint authorization token is a text string of 1-255 characters used by the BLE to authorize to and securely communicate with the BMC. This token is unique for each deployment.</p> <p>1-255</p>

Parameter	Description
ble-url <ble-url>	URL of the Meridian server to which the BLE sends monitoring data.
bootstrap-threshold <bootstrap-threshold>	<p>Configures number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP reboots.</p> <p>On the Mobility Conductor, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.</p> <p>1-65535</p> <p>8</p>
bridge-offload	Enables the hardware acceleration of bridge traffic.
clone <source>	Name of an existing AP system profile from which parameter values are copied.
console-enable	<p>Enables console port on the AP.</p> <p>enabled</p>
<pre>console-log-lvl {alerts critical debugging emergencies errors informational notifications warnings}</pre>	<p>Specifies the level of driver log prints sent to AP console. The description of different log levels are as follows:</p> <ul style="list-style-type: none"> ■ emergencies: To send driver log prints when system is unusable ■ alerts: To send driver log prints when Immediate action is needed ■ critical: To send

Parameter	Description
	<p>driver log prints when critical conditions exist</p> <ul style="list-style-type: none"> ■ errors: To send driver log prints when there are error conditions ■ warnings: To send driver log prints for warning conditions ■ notifications: To send driver log prints when a normal, but significant condition occurs ■ informational: To send driver log prints for informational messages ■ debugging: To send driver log prints for debugging messages <p>Do not change the console log level without prior supervision from the Aruba Technical Support team.</p> <p>emergencies</p>
disable-factory-reset	<p>Disables factory reset when the AP is operational.</p> <p>disabled</p>
dscp-to-dot1p-priority-mapping	<p>Configures semicolon-separated mapping between IP DSCP value and VLAN 802.1p priority.</p> <p>Format: <DSCP range/list (0-63)>:<802.1p value (0-7)></p> <p>Format Example: 24:4;32,34:3;45-56:1;57-60,62:7</p>

Parameter	Description
<pre>dns-domain <dns-domain></pre>	<p>Name of domain that is resolved by corporate DNS servers. Use this parameter when configuring split tunnel.</p>
<pre>double-encrypt</pre>	<p>This parameter applies only to remote APs. Use double encryption for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel. All other types of data traffic between the Mobility Conductor and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPsec tunnel.</p> <p>disabled</p>
<pre>driver-log-level {alerts critical debugging emergencies errors informational notifications warnings}</pre>	<p>Configures the level of driver log prints sent to syslog server. The description of different log levels are as follows:</p> <ul style="list-style-type: none"> ■ emergencies: To send driver log prints when system is unusable ■ alerts: To send driver log prints when Immediate action is needed ■ critical: To send driver log prints when critical conditions exist ■ errors: To send driver log prints when there are error conditions

Parameter	Description
	<ul style="list-style-type: none"> ■ warnings: To send driver log prints for warning conditions ■ notifications: To send driver log prints when a normal, but significant condition occurs ■ informational: To send driver log prints for informational messages ■ debugging: To send driver log prints for debugging messages <p>warnings</p>
<p>dual-5ghz-mode {automatic disabled enabled}</p>	<p>Mode for Dual 5GHz APs:</p> <ul style="list-style-type: none"> ■ automatic: Dual 5GHz Mode is enabled or disabled automatically. ■ disabled: Dual 5GHz mode is disabled. ■ enabled: both radios operate on 5GHz band. <p>The dual-5ghz-mode parameter is supported only on 340 Series (AP-344 and AP-345) access points. However, the automatic mode is not supported on AP-344 access points.</p>

Parameter	Description
	<p>For example, if the configuration for dual-5ghz-mode is set to automatic, AP-344 access points do not support a dynamic mode change. Users must manually set dual-5ghz-mode to Enabled if they require AP-344 access points to operate in the dual 5GHz mode.</p> <p>Additionally, users must purchase the required dual 5GHz external antenna.</p> <p>In a conductor-local or a stand-alone controller mode, automatic is treated as disabled. In a Mobility Conductor-Managed Device mode, automatic indicates that AirMatch determines when to modify the operating mode from dual band to the dual 5GHz mode.</p> <p>automatic</p>
<pre>dump-server <dump-server> (For versions prior to ArubaOS 8.4.0.0)</pre>	<p>(For debugging purposes) Specifies the server to receive a core dump generated when an AP process crashes.</p>
<pre>dump-collection-profile (ArubaOS 8.4.0.0 or later versions) {default profile-name}</pre>	<p>Specifies the profile for collecting core dump when an AP process crashes.</p>
<pre>clone</pre>	<p>Copies data from another dump collection profile.</p>
<pre>dynamic-pcap-interval</pre>	<p>Configures dynamic PCAP collection interval in minutes.</p> <p>0-30</p>

Parameter	Description
no	Deletes the command.
server-ip	Configures the server IP(v4/v6) for the dump collection.
server-password	Configures the server password for the dump collection.
server-path	Configures the server file path for the dump collection.
server-port	Configures the server port for the dump collection.
server-username	Configures the server username for the dump collection.
system-dump-enable	Enables the collection of system dump when an AP process crashes.
transfer-mode	Configures the Dump Transfer Mode.
transfer-enable	<p>Enables AP to transfer core dump to controller and server.</p> <p>NOTE: By default, the <code>transfer-enable</code> sub-parameter is enabled allowing the AP to transfer the core dump and when disabled the core dump is stored on the AP.</p>
flex-radio-mode {2.4GHz 2.4GHz-and-5GHz 5GHz }	<p>The mode for flexible radios. Use the following parameters:</p> <ul style="list-style-type: none"> ■ 2.4GHz—The radio operates on 2.4GHz. ■ 2.4GHz-and-5GHz—The radio operates on both 2.4GHz and 5GHz.

Parameter	Description
	<ul style="list-style-type: none"> ■ 5GHz—The radio operates on 5GHz.
<pre>flex-dual {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz}</pre>	<p>Enables the flex dual band support for an AP on stand-alone controllers. The flex dual band can be in one of the following three modes:</p> <ul style="list-style-type: none"> ■ 2.4GHz-and-6GHz—The radio 0 operates on 2.4 GHz and radio 1 operates on 6 GHz. ■ 5GHz-and-2.4GHz—The radio 0 operates on 5 GHz and radio 1 operates on 2.4 GHz. ■ 5GHz-and-6GHz—The radio 0 operates on 5 GHz and radio 1 operates on 6 GHz.
<pre>flex-dual-mode {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz Automatic}</pre>	<p>Enables the flex dual band support for an AP in a Mobility Master-Managed Device topology. The flex dual band can be in one of the following four modes:</p> <ul style="list-style-type: none"> ■ 2.4GHz-and-6GHz—The radio 0 operates on 2.4 GHz and radio 1 operates on 6 GHz. ■ 5GHz-and-2.4GHz—The radio 0 operates on 5 GHz and radio 1 operates on 2.4 GHz. ■ 5GHz-and-6GHz—The radio 0 operates on 5 GHz and radio 1 operates on 6 GHz. ■ Automatic—The radio 0 operates on 5GHz,

Parameter	Description
	radio 1 operates on 2.4GHz, and AirMatch will assign the operating mode dynamically.
gre-offload	HW acceleration of GRE traffic (for test purpose only) disabled
he-pooling-enable	Enables HE pooling. Disabling this parameter overrides Airmatch decision to include APs in HE pooling.
health-check	The AP Health check feature configured via the <code>health-check</code> parameters uses ping probes to check reachability and latency levels for the connection between the AP and the managed device. Recorded latency information appears in the output of the <code>show ap ip health-check</code> command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (<code>tmp</code> or <code>ap_hcm_log</code>) on the AP.
burst-size <size>	Number of probes to be sent during the probe frequency interval defined by the <code>frequency health-check</code> parameter. 1-16

Parameter	Description
	5
<pre>frequency <frequency></pre>	<p>Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the <code>burst-size</code> parameter during each frequency interval defined by this <code>frequency</code> parameter.</p> <p>10-300 10</p>
<pre>mode <mode></pre>	<p>Ping probe mode is the only mode currently supported by this feature.</p> <p>ping</p>
<pre>packet-size <packet-size></pre>	<p>The size, in bytes, of a ping datagram.</p> <p>10-2000 32</p>
<pre>report <report></pre>	<p>Number of seconds between health check reports sent from the AP to the controller. usage reports.</p> <p>60-3600 60</p>
<pre>retries <retries></pre>	<p>Number of times the attempts to resend a probe.</p> <p>1-10 3</p>

Parameter	Description
<pre>health-check-option</pre>	<p>Issue the <code>ap system-profile <profile> health-check-option</code> command to enable the AP Health check feature.</p> <p>disabled</p>
<pre>heartbeat-dscp <heartbeat-dscp></pre>	<p>Define the DSCP value of AP heartbeats. Use this feature to prioritize AP heartbeats and prevent the AP from losing connectivity with the Mobility Conductor over high-latency or low-bandwidth WAN connections.</p> <p>0-63</p> <p>0</p>
<pre>heartbeat-in <heartbeat-interval></pre>	<p>Set the interval between heartbeat messages between a remote or campus AP and its associated Mobility Conductor. An increase in the heartbeat interval increases the time it will take for an AP to detect the loss in connectivity to the Mobility Conductor, but can reduce internet bandwidth consumed by a remote AP.</p> <p>1-60</p> <p>1</p>
<pre>image-url <image-url></pre>	<p>Provide the image URL for an alternate AP image.</p>

Parameter	Description
ipm-enable	Enables the IPM system. To disable this feature, execute the <code>no ipm-enable</code> command. disabled
ipm-power-reduction-step-prio all	Sets up all the IPM power reduction steps.
ipm-power-reduction-step-prio ipm-step	Set IPM power and temperature reduction steps.
cpu_throttle_25	Configure this option to reduce the CPU frequency to 25%.
cpu_throttle_50	Configure this option to reduce the CPU frequency to 50%.
cpu_throttle_75	Configure this option to reduce the CPU frequency to 75%.
disable_alt_eth	Disables the second Ethernet port.
disable_pse1	Disable the first PSE port.
disable_pse2	Disable the second PSE port.
disable_usb	Disable the USB port.
radio_2ghz_chain_1x1 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 2.4 GHz chains to 1x1.
radio_1_chain_1x1 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 1 chains to 1x1.
radio_2ghz_chain_2x2 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 2.4 GHz chains to 2x2.
radio_1_chain_2x2 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 1 chains to 2x2.

Parameter	Description
radio_2ghz_chain_3x3 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 2.4 GHz chains to 3x3.
radio_1_chain_3x3 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 1 chains to 3x3.
radio_2ghz_disable (For versions prior to ArubaOS 8.11.0.0)	Configure this option to disable the 2.4 GHz radio band.
radio_1_disable (ArubaOS 8.11.0.0 or later versions)	Configure this option to disable radio 1.
radio_2ghz_power_3dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 2.4 GHz radio power by 3 dB from the maximum value.
radio_1_power_3dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 1 power by 3 dB from the maximum value.
radio_2ghz_power_6dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 2.4 GHz radio power by 6 dB from the maximum value.
radio_1_power_6dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 1 power by 6 dB from the maximum value.
radio_5ghz_2_chain_1x1 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the secondary 5 GHz radio chains to 1x1.
radio_2_chain_1x1 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 chains to 1x1.
radio_5ghz_2_chain_2x2 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the secondary 5 GHz radio chain to 2x2.

Parameter	Description
radio_2_chain_2x2 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 chains to 2x2.
radio_5ghz_2_chain_3x3 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the secondary 5 GHz radio chain to 3x3.
radio_2_chain_3x3 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 chains to 3x3.
radio_5ghz_2_disable (For versions prior to ArubaOS 8.11.0.0)	Configure this option to disable the secondary 5 GHz radio.
radio_2_disable (ArubaOS 8.11.0.0 or later versions)	Configure this option to disable radio 2.
radio_5ghz_2_power_3dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 5 GHz radio power by 3 dB from the maximum value.
radio_2_power_3dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 power by 3 dB from the maximum value.
radio_5ghz_2_power_6dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 5 GHz radio power by 6 dB from the maximum value.
radio_2_power_6dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 power by 6 dB from the maximum value.
radio_5ghz_chain_1x1 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chains to 1x1.
radio_0_chain_1x1 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 1x1.
radio_5ghz_chain_2x2 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chains to 2x2.

Parameter	Description
radio_0_chain_2x2 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 2x2.
radio_5ghz_chain_3x3 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chains to 3x3.
radio_0_chain_3x3 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 3x3.
radio_5ghz_chain_4x4 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chain to 4x4.
radio_0_chain_4x4 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 4x4.
radio_5ghz_chain_5x5 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chains to 5x5.
radio_0_chain_5x5 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 5x5.
radio_5ghz_chain_6x6 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chain to 6x6.
radio_0_chain_6x6 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 6x6.
radio_5ghz_chain_7x7 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 5 GHz chain to 7x7.
radio_0_chain_7x7 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 0 chains to 7x7.
radio_5ghz_disable (For versions prior to ArubaOS 8.11.0.0)	Configure this option to disable the 5 GHz radio band.
radio_0_disable (ArubaOS 8.11.0.0 or later versions)	Configure this option to disable radio 0.

Parameter	Description
radio_5ghz_power_3dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 5 GHz radio power by 3 dB from the maximum value.
radio_0_power_3dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 0 power by 3 dB from the maximum value.
radio_5ghz_power_6dB (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 5 GHz radio power by 6 dB from the maximum value.
radio_0_power_6dB (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 0 power by 6 dB from the maximum value.
radio_6ghz_chain_1x1 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 6 GHz chains to 1x1.
radio_2_chain_1x1 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 2 chains to 1x1.
radio_6ghz_chain_2x2 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 6 GHz chains to 2x2.
radio_2_chain_2x2 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 2 chains to 2x2.
radio_6ghz_chain_3x3 (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce 6 GHz chains to 3x3.
radio_2_chain_3x3 (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce radio 2 chains to 3x3.
radio_6ghz_disable (For versions prior to ArubaOS 8.11.0.0)	Configure this option to disable the 6 GHz radio.
radio_2_disable (ArubaOS 8.11.0.0 or later versions)	Configure this option to disable radio 2.

Parameter	Description
<code>radio_6ghz_power_3dB</code> (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 6 GHz radio power by 3 dB from the maximum value.
<code>radio_2_power_3dB</code> (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 power by 3 dB from the maximum value.
<code>radio_6ghz_power_6dB</code> (For versions prior to ArubaOS 8.11.0.0)	Configure this option to reduce the 6 GHz radio power by 6 dB from the maximum value.
<code>radio_2_power_6dB</code> (ArubaOS 8.11.0.0 or later versions)	Configure this option to reduce the radio 2 power by 6 dB from the maximum value.
<code>priority <priority></code>	Sets the priorities for IPM power reduction steps.
<code>itm-enable</code>	<p>Enables the intelligent temperature monitoring system. If enabled, the temperature is dynamically controlled and the AP is allowed to cool down. To disable this feature, issue the <code>no itm-enable</code> command.</p> <p>NOTE:</p> <ul style="list-style-type: none"> ■ This feature can be enabled only when the IPM feature is enabled. ■ This feature is supported only on AP-505H, AP-518, 570 Series, and 580 Series access points. <p>disabled</p>

Parameter	Description
led-mode	<p>The operating mode for the AP LEDs. This option is available on all 802.11n indoor AP platforms.</p> <p>normal</p>
normal	Display LEDs in normal mode.
off	Turn off all LEDs.
led-override	<p>Override the LED action for single-LED APs in normal LED operating mode. If enabled, this feature disables the LED auto-turn-off function.</p> <p>disabled</p>
lms-hold-down-period	<p>Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.</p> <p>1-3600</p> <p>600</p>
lms-ip <lms-ip>	<p>In multi-controller networks, this parameter specifies the IP address of the LMS—the managed device—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Conductor.</p>

Parameter	Description
	<p>When using redundant managed device as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions. If the LMS-IP is blank, the access point will remain on the managed device that it finds using methods like DNS or DHCP. If an IP address is configured for the LMS IP parameter, the AP will be immediately redirected to the managed device at that address.</p>
<pre>lms-ipv6 <lms-ipv6></pre>	<p>In multi-controller IPv6 networks, specify the IPv6 address of the LMS—the managed device—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Conductor. When using redundant managed device as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions.</p>

Parameter	Description
<p>lms-ping-interval <lms-ping-interval></p>	<p>Specifies the interval at which application level ping needs to be sent to managed device to check the reachability. Applicable only for Remote AP. If this parameter is changed, UDP session timeout on an intermediate router which performs the NAT function should be set accordingly. The preferred timeout value is (lms-ping-interval + 30 seconds).</p> <p>10-60 20</p>
<p>lms-preemption</p>	<p>Automatically reverts to the primary LMS IP address when it becomes available.</p> <p>disabled</p>
<p>maintenance-mode</p>	<p>Enable or disable AP maintenance mode. This setting is useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to NMS systems or network operations centers when deploying, maintaining, or upgrading the network. The Mobility Conductor still generates debug syslog messages if debug logging is enabled.</p> <p>disabled</p>

Parameter	Description
<pre>max-request-retries <max-request-retries></pre>	<p>Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.</p> <p>1-65535 10</p>
<pre>mcast-aggr</pre>	<p>Enable multicast aggregation at AP.</p> <p>disabled</p>
<pre>mcast-aggr-allowed-vlan <vlan-list></pre>	<p>Enable list of VLANs where AP multicast aggregation is allowed.</p> <p>disabled</p>
<pre>mgmt-dscp <mgmt-dscp></pre>	<p>Sets the DSCP value of AP management packets.</p> <p>0-63</p>
<pre>mtu</pre>	<p>MTU, in bytes, on the wired link for the AP.</p> <p>1024-1578</p>
<pre>native-vlan-id <native-vlan-id></pre>	<p>Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).</p> <p>1</p>
<pre>no</pre>	<p>Negates any configured parameter.</p>
<pre>number-ipsec-retries <number_ipsec_retries></pre>	<p>The number of times the AP will attempt to recreate an IPsec tunnel with the Mobility Conductor before the AP will reboot. A value of 0 disables the reboot.</p>

Parameter	Description
	1-1000 85
rap-bw-resv-1 acl <aclname> [priority <priority>]	Session ACLs with uplink bandwidth reservation in Kbps. You can specify up to three session ACLs to reserve uplink bandwidth. The sum of the three uplink bandwidths should not exceed the rap-bw-total value. BW value is in Kbps. Optionally, you can specify the priority for class 1, class 2, and class 3 traffic.
rap-bw-resv-2 acl <aclname> <bwvalue> [priority <priority>]	
rap-bw-resv-3 acl <aclname> [priority <priority>]	
rap-bw-total <rap-bw-total>	This is the total reserved uplink bandwidth (in Kbps).
rap-corp-dns-server <ipv4 address>	IPv4 address of the Corporate DNS server
rap-corp-dns-server_ ipv6 <ipv6 address>	IPv6 address of the Corporate DNS server
rap-dhcp-default-router <rap-dhcp-default-router>	IP address for the default DHCP router. 192.168.11.1
rap-dhcp-dns-server <rap-dhcp-dns-server>	IP address of the DNS server. 192.168.11.1
rap-dhcp-lease <rap-dhcp-lease>	The amount of days that the assigned IP address is valid for the client. Specify the lease in <days>. 0 indicates the IP address is always valid; the lease does not expire. 0-30 0

Parameter	Description
<pre>rap-dhcp-pool-end <rap-dhcp-pool-end></pre>	<p>Configures a DHCP pool for remote APs. This is the last IP address of the DHCP pool.</p> <p>192.168.11.254</p>
<pre>rap-dhcp-pool-netmask <rap-dhcp-pool-netmask></pre>	<p>Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool.</p> <p>255.255.255.0</p>
<pre>rap-dhcp-pool-start <rap-dhcp-pool-start></pre>	<p>Configures a DHCP pool for remote APs. This is the first IP address of the DHCP pool.</p> <p>192.168.11.2</p>
<pre>rap-dhcp-server-id <rap-dhcp-server-id></pre>	<p>IP address used as the DHCP server identifier.</p> <p>192.168.11.1</p>
<pre>rap-dhcp-server-vlan <rap-dhcp-server-vlan></pre>	<p>VLAN ID of the remote AP DHCP server used if the Mobility Conductor is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable.</p>
<pre>rap-gre-mtu <rap-gre-mtu></pre>	<p>Configures the maximum size of the GRE packets exchanged between a Remote AP and the Mobility Conductor.</p> <p>1024-1578 1200</p>
<pre>rap-local-network-access</pre>	<p>Enable or disable local network access across VLANs in a Remote AP.</p>

Parameter	Description
	disabled
<pre>recovery-mode {legacy auto}</pre>	<p>Select either the legacy recovery mode or the auto mode (fast recovery).</p> <ul style="list-style-type: none"> ■ legacy— On detecting a firmware assert, the AP transfers the core-dump to the managed device and executes an AP reboot. ■ auto—On detecting a firmware assert, the AP executes the fast recovery process in the radio affected instead of rebooting the AP. This reduces the downtime of the AP in the network. If the AP detects a core dump with a valuable information during a firmware assert, then it transfers the core dump to the managed device and the AP reboots. <p>The fast recovery mode for 530 Series and 550 Series access points is disabled by default.</p> <p>legacy</p>
<pre>request-retry-interval <request-retry-interval></pre>	<p>Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.</p> <p>1-65535</p>

Parameter	Description
	10
rf-band {a g}	For APs that support both <i>a</i> and <i>b/g</i> RF bands, RF band in which the AP should operate: <ul style="list-style-type: none"> ■ g = 2.4 GHz ■ a = 5 GHz g
rtls-server	Enables the AP to send RFID tag information to an RTLS server.
ip-or-dns	IPv4/IPv6 address or the DNS of the RTLS server to which location reports are sent.
port	Port number on the server to which location reports are sent.
key	Shared secret key.
station-message-frequency	Indicates how often packets are sent to the server.\ 1-3600 30
[include-unassoc-sta {enable disable}]	RTLS station reporting includes information for APs and the clients that the AP has detected. If you include the <code>include-unassoc-sta</code> parameter, the station reports will also include information about clients not associated to any AP. By default, unassociated clients are not included in station reports.

Parameter	Description
	disabled
rtls-server-compat_mode	The compatibility mode controls the format of tag frames forwarded to the RTLS server. Enabling this mode will enable legacy format (includes a 2 byte padding), and disabling this mode will remove the padding. The tag frame format will be the same across all AP models.
secondary-master/secondary-conductor <secondary-master>/<secondary-conductor>	Assigns a remote AP as a secondary Mobility Conductor in the event the primary Mobility Conductor can not be reached.
sesImagotag-esl-channel	Sets the channel of SES-imagotag ESL Radio. There are 12 pre-defined, independent radio channels. Channel 0 to 10 and 127 are valid channels and channel 11 is an invalid channel. The recommended channels are 3, 5, 8, 9, and 10 as they connect faster. These channels do not correspond to standard 802.11 channels. 0-10 and 127
sesimagotag-esl-radio-coexistence	Enables radio co-existence features between SES-imagotag ESL radio and 2.4 G WiFi radio

Parameter	Description
sesimagotag-esl-server	Sets the FQDN of SES-imagotag ESL Server. Server name takes priority over IP address. If server name is configured, IP address will not take effect. If server name is not configured, IP address takes effect. To disable SES-imagotag ESL server, do not configure server name and IP address.
sesimagotag-esl-serverip	Sets the IP Address of SES-imagotag ESL Server. Adding server IP addresses allows bulk management and control of multiple servers at the same time. Starting from ArubaOS 8.7.1.9, a new option to configure the port number for SES Imagotag dongles is introduced. Custom port can be set using the port option. The port setting is optional. The domain name configuration should be followed by a colon and the port number :-<port number> . If the port number is not defined the default port will be used by SES Imagotag dongles. For example, (host) [mynode] (AP system profile "test")sesimagotag-esl-server arubanetworks.com:64104
sesimagotag-esl-tls-auth	Allows AP to authenticate with SES-Imagotag ESL server.

Parameter	Description
<pre>sesimagotag-esl-tls-fqdn-verify</pre>	<p>Allows AP to verify TLS FQDN</p>
<pre>session-acl <session-acl></pre>	<p>Session ACL configured with the ip access-list session command. This parameter requires the PEFNG license. If PEFNG license is installed, ap uplink-acl is applied, else no ACL is applied.</p>
<pre>slow_timer_recovery</pre>	<p>If you enable this option, ArubaOS checks for a slow CPU timer, and if it detects an issue, it restarts the AP without logging a reason for the reboot. This feature is supported on RAP-108 or RAP-109 access points.</p> <p>disabled</p>
<pre>spanning-tree</pre>	<p>Enables the spanning-tree protocol.</p> <p>disabled</p>
<pre>split-5ghz-mode</pre>	<p>Set mode for split-5GHz capable APs from one of the following:</p> <ul style="list-style-type: none"> ▪ Automatic : Split-5GHz radio mode is enabled or disabled automatically ▪ Disabled: Split-5GHz radio mode will be disabled. ▪ Enabled: 8x8:8SS 5GHz radio will be split to 2 4x4:4SS 5GHz radios.

Parameter	Description
syscontact	SNMP system contact information.
telnet	Enables or disables telnet or SSH to the AP. Telnet is enabled on an AP running ArubaOS 8.6.0.0 or previous versions. SSH is enabled on an AP running ArubaOS 8.7.0.0 firmware version. disabled
wids-ampdu-optimization	Enables or disables WIDS aggregate MPDU optimization. disabled
wired-poe-bounce-interval <wired-poe-bounce-interval>	Configures the down time of PoE wired port after the AP fails over to backup cluster or falls back to primary cluster. 0-60 secs 0 NOTE: The port bounce feature is disabled when the default value is 0.
wired-port-bounce-interval <wired-port-bounce-interval>	Configures the down time of Ethernet link wired port after the AP fails over to backup cluster or falls back to primary cluster. 0-60 secs 0 NOTE: The port bounce feature is disabled when the default value is 0.

Example

The following command configures the Dual 5GHz mode option for 340 Series access points:

```
(host) [mynode] (config) #ap system profile <profile-name>
(host) [mynode] (AP system profile "<profile-name>") #dual-5ghz-mode enabled
```

The following commands configure LACP and AP LACP LMS map information settings:

```
(host) [mynode] (config) #ap system-profile LACP
(host) [mynode] (AP system profile "LACP") #lms-ip 192.0.2.1
(host) [mynode] (AP system profile "LACP") #exit
(host) [mynode] (config) #ap-lacp-striping-ip
(host) [mynode] (AP LACP LMS map information) #striping-ip 192.0.2.2 lms
192.0.2.1
(host) [mynode] (AP LACP LMS map information) #aplacp-enable
```

For more information on configuring LACP support, including important pre-deployment considerations and troubleshooting information, refer to the *ArubaOS User Guide*. It is recommended not to configure GRE striping IP address for stand-alone controller deployments.

The following command removes one IPM step or priority from the AP system profile, "default":

```
(host) [mynode] (config) #ap system-profile default
(host) [mynode] (AP system profile "default") #no ipm-power-reduction-step-
prio ipm-step cpu_throttle_50
```

The following command removes all IPM priorities set for an AP system profile:

```
(host) [mynode] (AP system profile "default") #no ipm-power-reduction-step-
prio all
```

The following commands configure the recovery mode parameter for 300 Series access points:

```
(host) [mynode] (config) #ap system-profile <profile-name>
(host) [mynode] (AP system profile "<profile-name>") #recovery-mode auto
```

The following commands configure the wired port downtime for both Ethernet link and PoE:

```
(host) [mynode] (config)#ap system-profile <profile-name>
(host) [mynode] (AP system profile "<profile-name>") # wired-poe-bounce-
interval <wired-poe-bounce-interval>
(host) [mynode] (AP system profile "<profile-name>") # wired-port-bounce-
interval <wired-port-bounce-interval>
(host) [mynode] (AP system profile "<profile-name>") # write memory
```

Command History

Release	Modification
ArubaOS 8.11.0.0	<p>The following modifications were introduced:</p> <ul style="list-style-type: none"> ■ The following new parameters were added: <ul style="list-style-type: none"> ● <code>flex-dual {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz}</code> ● <code>flex-dual-mode {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz Automatic}</code> ■ The following changes were made to the <code>ipm-power-reduction-step-prio ipm-step</code> parameter: <ul style="list-style-type: none"> ● Replaced <code>radio_2ghz_chain_1x1</code> with <code>radio_1_chain_1x1</code> ● Replaced <code>radio_2ghz_chain_2x2</code> with <code>radio_1_chain_2x2</code> ● Replaced <code>radio_2ghz_chain_3x3</code> with <code>radio_1_chain_3x3</code> ● Replaced <code>radio_2ghz_disable</code> with <code>radio_1_disable</code> ● Replaced <code>radio_2ghz_power_3dB</code> with <code>radio_1_power_3dB</code> ● Replaced <code>radio_2ghz_power_6dB</code> with <code>radio_1_power_6dB</code> ● Replaced <code>radio_5ghz_2_chain_1x1</code> with <code>radio_2_chain_1x1</code> ● Replaced <code>radio_5ghz_2_chain_2x2</code> with <code>radio_2_chain_2x2</code> ● Replaced <code>radio_5ghz_2_chain_3x3</code> with <code>radio_2_chain_3x3</code> ● Replaced <code>radio_5ghz_2_disable</code> with <code>radio_2_disable</code> ● Replaced <code>radio_5ghz_2_power_3dB</code> with <code>radio_2_power_3db</code> ● Replaced <code>radio_5ghz_2_power_6dB</code> with <code>radio_2_power_6db</code> ● Replaced <code>radio_5ghz_chain_1x1</code> with <code>radio_0_chain_1x1</code> ● Replaced <code>radio_5ghz_chain_2x2</code> with <code>radio_0_chain_2x2</code> ● Replaced <code>radio_5ghz_chain_3x3</code> with <code>radio_0_chain_3x3</code>

Release	Modification
	<ul style="list-style-type: none"> ● Replaced <code>radio_5ghz_chain_4x4</code> with <code>radio_0_chain_4x4</code> ● Replaced <code>radio_5ghz_chain_5x5</code> with <code>radio_0_chain_5x5</code> ● Replaced <code>radio_5ghz_chain_6x6</code> with <code>radio_0_chain_6x6</code> ● Replaced <code>radio_5ghz_chain_7x7</code> with <code>radio_0_chain_7x7</code> ● Replaced <code>radio_5ghz_disable</code> with <code>radio_0_disable</code> ● Replaced <code>radio_5ghz_power_3dB</code> with <code>radio_0_power_3dB</code> ● Replaced <code>radio_5ghz_power_6dB</code> with <code>radio_0_power_6dB</code> ● Replaced <code>radio_6ghz_chain_1x1</code> with <code>radio_2_chain_1x1</code> ● Replaced <code>radio_6ghz_chain_2x2</code> with <code>radio_2_chain_2x2</code> ● Replaced <code>radio_6ghz_chain_3x3</code> with <code>radio_2_chain_3x3</code> ● Replaced <code>radio_6ghz_disable</code> with <code>radio_2_disable</code> ● Replaced <code>radio_6ghz_power_3dB</code> with <code>radio_2_power_3dB</code> ● Replaced <code>radio_6ghz_power_6dB</code> with <code>radio_2_power_6dB</code> ■ The <code>flex-radio-mode {2.4GHz 2.4GHz-and-5GHz 5GHz}</code> parameter was removed for stand-alone controllers only (ArubaOS 8.11.0.0 or later versions).
ArubaOS 8.10.0.0	<p>The following modifications were introduced:</p> <ul style="list-style-type: none"> ■ The following sub-parameters were added to the <code>ipm-power-reduction-step-prio ipm-step</code> parameter: <ul style="list-style-type: none"> ● <code>radio_2ghz_disable</code> ● <code>radio_5ghz_disable</code> ● <code>radio_5ghz_2_chain_1x1</code> ● <code>radio_5ghz_2_chain_2x2</code> ● <code>radio_5ghz_2_chain_3x3</code>

Release	Modification
	<ul style="list-style-type: none"> ● radio_5ghz_2_disable ● radio_5ghz_2_power_3dB ● radio_5ghz_2_power_6dB ● radio_6ghz_chain_1x1 ● radio_6ghz_chain_2x2 ● radio_6ghz_chain_3x3 ● radio_6ghz_disable ● radio_6ghz_power_3dB ● radio_6ghz_power_6dB ■ The sub-parameter transfer-enable was added to the dump-collection-profile parameter .
ArubaOS 8.9.0.0	<p>The following parameters were modified: All instances of master have been replaced with conductor. All instances of secondary-master have been replaced with secondary-conductor.</p>
ArubaOS 8.8.0.0	<p>The following parameters were added:</p> <ul style="list-style-type: none"> ■ wired-poe-bounce-interval <wired-poe-bounce-interval> ■ wired-port-bounce-interval <wired-port-bounce-interval> ■ sesImagotag-esl-radio-coexistence ■ sesImagotag-esl-tls-auth ■ sesImagotag-esl-tls-fqdn-verify <p>The value, 127, was added to the sesImagotag-esl-channel parameter.</p>
ArubaOS 8.7.1.9	<p>The sesimagotag-esl-serverip parameter was enhanced.</p>
ArubaOS 8.7.0.0	<p>The following parameters were added:</p> <ul style="list-style-type: none"> ■ disable-factory-reset ■ he-pooling-enable ■ itm-enable <p>The following parameters were modified:</p> <ul style="list-style-type: none"> ■ telnet ■ itm-enable ■ ipm-power-reduction-step-prio ipm-step

Release	Modification
ArubaOS 8.6.0.0	The <code>sesimagotag-esl-server</code> parameter was added.
ArubaOS 8.5.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>rap-corp-dns-server <ipv4 address></code> ■ <code>rap-corp-dns-server_ ipv6 <ipv6 address></code>
ArubaOS 8.4.0.0	The following modifications were introduced: <ul style="list-style-type: none"> ■ The IPv6 address support was added to the <code>ip-or-dns</code> parameter. ■ The <code>ap-usb-power-mode</code> and <code>wids-ampdu-optimization</code> parameters were added. ■ The <code>sesImagotag-esl-channel</code> and <code>sesImagotag-esl-serverip</code> parameters were added. ■ The <code>ap-usb-power-override</code> parameter was deprecated. The following parameters were added: <ul style="list-style-type: none"> ■ <code>radio_5ghz_chain_4x4</code> ■ <code>radio_5ghz_chain_5x5</code> ■ <code>radio_5ghz_chain_6x6</code> ■ <code>radio_5ghz_chain_7x7</code> ■ The <code>dump-server <dump-server></code> parameter was deprecated. ■ The <code>dump-collection-profile {default profile-name}</code> parameter was introduced.
ArubaOS 8.3.0.0	The following new parameters were added: <ul style="list-style-type: none"> ■ <code>dual-5ghz-mode</code> ■ <code>recovery-mode</code> ■ <code>ap-deploy-hour</code>
ArubaOS 8.2.0.0	<ul style="list-style-type: none"> ■ The <code>all</code> sub-parameter was added to the <code>ipm-power-reduction-step-prio</code> parameter. ■ The <code>no ipm-power-reduction-step-prio ipm-step <ipm-step> priority <priority number></code> parameter was changed to <code>no ipm-power-reduction-step-prio ipm-step <ipm-step></code>. ■ The <code>flex-radio-mode</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ap test

```
ap test
  airmatch
  ap-name
  bss-termination
  dot11k-force-beacon-request
  dot11k-force-link-measurement-request
  dot11k-force-tsm-request
  dot11v-force-bss-transition
  force_send_delts
  ip-addr
  ip6-addr
  netdest
  network-check
  rebootstrap
  remote-dot11v-force-bss-transition
  wan
```

Description

Execute this command to get the test results in an AP.

Parameter	Description
ap test	Run test command on AP.
ap-name bar-retries bar-times	Name of the access point.
bss-termination	Trigger timed BSS-termination, sending BTM-requests to MBO-STAs.
dot11k-force-beacon-request sta <sta_mac>	Test force sending 802.11 Beacon Report Request frame.
dot11k-force-link-measurement-request sta <sta_mac>	Test force sending 802.11 Link Measurement Request frame.
dot11k-force-tsm-request sta <sta_mac>	Test force sending TSM Report Request frame.
dot11v-force-bss-transition sta <sta_mac>	Test force sending BSS Transition Mgmt Request frame.

Parameter	Description
<code>force_send_delts</code>	Force sending DELTS to the client.
<code>ip-addr</code>	IP Address of Access Point.
<code>ip6-addr</code>	IPv6 address of Access Point.
<code>netdest</code>	Trigger netdestination config push.
<code>network-check</code>	Check the network.
<code>rebootstrap ap-name ip-addr ip6-addr</code>	Rebootstrap AP.
<code>remote-dot11v-force-bss-transition</code>	Test force sending BSS Transition Management Request frame.
<code>wan down up</code>	Wan link test command. <ul style="list-style-type: none"> ■ down — Trigger wan down event. ■ up — Trigger wan up event.

Example

The following command displays different results of AP-related tests:

```
(host) [mynode] #ap test
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

apugr

```
apugr
  act part <partition>
  add ap-name <ap-name>
  move ap-name <ap-name> target <target>
```

Description

This command can be executed for cluster upgrade.

Parameter	Description
act	Active upgrade preload ap.
part <partition>	AP preload partition.
add	Adds upgrade preload AP.
ap-name <ap-name>	Name of the AP.
move	Moves an AP to another target
ap-name <ap-name>	Name of the AP.
target <target>	Ip address of the target controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Conductor.

ap usb-acl-prof

```
ap usb-prof default | {<profile-name> clone | no | rule vendor <vendor> action <action>}
```

Description

This command is used to create a AP USB ACL profile.

Parameter	Description
default	Name of the default AP USB ACL profile.
<profile-name>	Name of the AP USB ACL profile.
clone	Copy AP USB ACL profile data from another AP USB ACL profile.
no	Negate any configured parameter.
rule	USB access rule.
vendor <vendor>	Name of USB vendor. Available options are: <ul style="list-style-type: none">■ Alcatel-L800■ Amberbox-detector■ Amberbox-gateway■ C-motech-CNU-680■ EpiValley-SEC-8089■ Franklin-u770-u772■ Franklin-U300■ Franklin-U301■ Franklin-U600■ Fujisoft■ Globetrotter-ICON-225■ Globetrotter-ICON-322■ HanShow■ Huawei-3276s-150■ Huawei-D41HW■ Huawei-E1552■ Huawei-E157■ Huawei-E160■ Huawei-E169-E180-E220■ Huawei-E170-E272-E220■ Huawei-E173■ Huawei-E1731-177DT06■ Huawei-E1750■ Huawei-E176-E176G-E1553■ Huawei-E1762■ Huawei-E180■ Huawei-E180-E1692-E1762

Parameter	Description
	<ul style="list-style-type: none"> ■ Huawei-E1820e ■ Huawei-E220 ■ Huawei-E261 ■ Huawei-E3131 ■ Huawei-E3272s-153 ■ Huawei-E3276 ■ Huawei-E3276s-500 ■ Huawei-E3372 ■ Huawei-E3372h-153-hil ■ Huawei-E3372h-153-modem ■ Huawei-E352s-5 ■ Huawei-E353 ■ Huawei-E353-E1750-E367 ■ Huawei-E367 ■ Huawei-E3765 ■ Huawei-E392 ■ Huawei-e398 ■ Huawei-E8372 ■ Huawei-EC150 ■ Huawei-EC167 ■ Huawei-HWD12-LTE ■ Huawei-K3770 ■ Huawei-K3772 ■ Huawei-K4505 ■ Huawei-K4510 ■ Huawei-K4605 ■ Huawei-K5150 ■ Huawei-K5160 ■ Huawei-KDDI-DATA07 ■ Icon-452 ■ Longcheer-WM72 ■ Netgear-340u ■ Netgear-341u ■ Novatel-MC545 ■ Novatel-MC551L ■ Novatel-MiFi-2200 ■ Novatel-Ovation-U727 ■ Novatel-U620L ■ Novatel-U720 ■ Novatel-U727 ■ Novatel-U760-Sprint ■ Novatel-U760-Virgin ■ NTT-DoCoMo-L-02A ■ NTT-DoCoMo-L-02C ■ NTT-DoCoMo-L-05A ■ NTT-DoCoMo-L-08C ■ Pantech-UM150 ■ Pantech-UM175 ■ Pantech-UM190 ■ Pantech-UML290 ■ Pantech-UML295

Parameter	Description
	<ul style="list-style-type: none"> ■ Pantech-UML295-cold ■ Qualcomm-SXC-1080 ■ SES-Imagotag-021 ■ Sierra-250U ■ Sierra-305-308 ■ Sierra-306-308-503-312U ■ Sierra-313u ■ Sierra-320U ■ Sierra-330U ■ Sierra-598 ■ Sierra-881U ■ Sierra-885 ■ Sierra-Compass-597 ■ Sierra-Compass-885 ■ Sierra-Tstick-C597 ■ SIMTech ■ Solu-M-SLG-DM101 ■ UGM1831 ■ UMG181 ■ Utstarcom-UM100C ■ ZTE-3565 ■ ZTE-AC2726 ■ ZTE-AC2736 ■ ZTE-AC3781 ■ ZTE-Fivespot ■ ZTE-K4505-z ■ ZTE-MF110 ■ ZTE-MF180-HSDPA ■ ZTE-MF190-Egypt ■ ZTE-MF190-India ■ ZTE-MF190-Thailand ■ ZTE-MF591 ■ ZTE-MF633-MF636 ■ ZTE-MF637-MF656 ■ ZTE-MF668 ■ ZTE-MF683-HSDPA ■ ZTE-MF79S ■ ZTE-MF820 ■ ZTE-MF820D ■ ZTE-MF823 ■ ZTE-MF825C ■ ZTE-MF831 ■ ZTE-MF832S ■ ZTE-MF832U ■ ZTE-MF832U-Zero
<p>action <vendor></p>	<p>Action to perform is name of USB vendor matches. Available options are:</p> <ul style="list-style-type: none"> ■ deny - Access to USB device is denied ■ permit - Access to USB device is refused

Example

The following command creates a USB ACL profile named sample-usb-acl-profile with rule to permit USB devices from HanShow:

```
(host) [mynode] (config) #ap usb-acl-prof sample-usb-acl-profile
(host) (mynode) (AP USB ACL Profile "sample-usb-acl-profile") #rule vendor
HanShow action permit
```

Related Commands

Command	Description
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
show ap usb-prof	Shows configuration for AP USB profile.
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.
ap usb-profile	Configures AP USB profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable Mode.

ap usb-profile

ap usb-profile default | {<profile-name> clone | no | usb-acl-profile}

Description

This command is used to create a AP USB profile.

Parameter	Description
default	Name of the default AP USB profile.
<profile-name>	Name of the AP USB profile.
clone	Copy AP USB profile data from another AP USB profile.
no	Negate any configured parameter.
usb-acl-profile	Apply USB ACL profile to AP USB profile.

Example

The following command creates an AP USB profile named sample-ap-usb-profile and applies a USB ACL profile named sample-usb-acl-profile to it:

```
(host) [mynode] (config) #ap usb-profile sample-ap-usb-profile
(host) (mynode) (AP USB profile "sample-ap-usb-profile") #usb-acl-profile
sample-usb-acl-profile
```

Related Commands

Command	Description
show ap usb-prof	Shows configuration for AP USB profile.
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.
ap usb-acl-prof	Configures AP USB ACL profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable Mode.

ap wake-up

```
ap wake-up
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  mac-list <mac_list>
  wired-mac <wired_mac>
```

Description

This command is used to wake up APs from the deep-sleep mode.

Parameter	Description
ap-name	Name of an AP.
ip-addr	IP address of AP.
ip6-addr	IPv6 address of AP.
mac-list	Semicolon separated MAC address list. The maximum characters supported is 250.
wired-mac	The MAC address of an AP.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ap wifi-uplink-profile

```
ap wifi-uplink-profile {default | <profile-name>}
  allowed band {a | g | all}
  bssid <bssid>
  clone {default | <source> }
  essid <essid>
  no
  opmode {opensystem | personal | static-wep}
  wepkey1 <wepkey1>
  wepkey2 <wepkey2>
  wepkey3 <wepkey3>
  wepkey4 <wepkey4>
  weptxkey <weptxkey>
  wpa-hexkey <wpa-hexkey>
  wpa-passphrase <wpa-passphrase>
```

Description

This command configures a Wi-Fi uplink profile. When both wpa-hexkey and wpa-passphrase parameters are configured, wpa-hexkey takes precedence.

Parameter	Description
ap wifi-uplink-profile <profile-name>	Name of this instance of the profile. The name must be 1-63 characters.
allowed band {a g all}	The radio band(s) on which the Wi-Fi uplink is used. Select one of the following options: <ul style="list-style-type: none">■ a: 802.11a band only (5 GHz)■ g: 802.11g band only (2.4 GHz)■ all: Both 802.11a and 802.11g bands (5 GHz and 2.4 GHz) all
bssid <bssid>	Name of the required BSSID to which the client is associated.
clone	Copies data from another Wi-Fi uplink profile.
essid <essid>	Name of the required ESSID to which the client is associated.
no	Negates any configured parameter.
opmode	Name of the data encryption mode. Select one of the following modes: <ul style="list-style-type: none">■ opensystem—No authentication or encryption.■ personal—A wildcard mode that matches several PSK mode key management suites and cipher suites,

Parameter	Description
	<p>including WPA-PSK-TKIP, WPA-PSK-AES, WPA2-PSK-TKIP and WPA2-PSK-AES.</p> <ul style="list-style-type: none"> ■ static-wep—WEP with static keys. <p>NOTE: The static-wep opmode is no longer supported from ArubaOS 8.11.0.0 onwards.</p> <p>opensystem</p>
wepkey1 <wepkey1>	<p>The first static WEP key associated with the key index. Can be 10 or 26 hex characters in length.</p> <p>NOTE: The wepkey1 <wepkey1> parameter is no longer supported from ArubaOS 8.11.0.0 onwards.</p>
wepkey2 <wepkey2>	<p>The second static WEP key associated with the key index. Can be 10 or 26 hex characters in length.</p> <p>NOTE: The wepkey2 <wepkey2> parameter is no longer supported from ArubaOS 8.11.0.0 onwards.</p>
wepkey3 <wepkey3>	<p>The third static WEP key associated with the key index. Can be 10 or 26 hex characters in length.</p> <p>NOTE: The wepkey3 <wepkey3> parameter is no longer supported from ArubaOS 8.11.0.0 onwards.</p>
wepkey4 <wepkey4>	<p>The fourth static WEP key associated with the key index. Can be 10 or 26 hex characters in length.</p> <p>NOTE: The wepkey4 <wepkey4> parameter is no longer supported from ArubaOS 8.11.0.0 onwards.</p>
weptxkey <weptxkey>	<p>The key index to specify which static WEP key is to be used. Can be 1, 2, 3, or 4.</p> <p>1</p> <p>NOTE: The weptxkey <weptxkey> parameter is no longer supported from ArubaOS 8.11.0.0 onwards.</p>
wpa-hexkey <wpa-hexkey>	<p>The WPA Pre-Shared Key (PSK). This key must be of 64 hexadecimal characters.</p>
wpa-passphrase <wpa-passphrase>	<p>The WPA password that generates the PSK. The passphrase must be between 8–63 characters, inclusive</p>

Example

The following commands create a Wi-Fi uplink profile:

```
(host) [mynode] (config) # ap wifi-uplink-profile test-uplink
(host) [mynode] (WiFi uplink profile "test-uplink") # essid uplink-new
(host) [mynode] (WiFi uplink profile "test-uplink") # wpa-passphrase *****
(host) [mynode] (WiFi uplink profile "test-uplink") # opmode personal
(host) [mynode] (WiFi uplink profile "test-uplink") # exit
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The following parameters were deprecated: <ul style="list-style-type: none"> ▪ static-wep under opmode ▪ wepkey1 <wepkey1> ▪ wepkey2 <wepkey2> ▪ wepkey3 <wepkey3> ▪ wepkey4 <wepkey4> ▪ weptxkey <weptxkey>
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ap wipe out flash

```
ap wipe out flash
  ap-name <ap-name>
  ip-addr <ip-addr>
```

Description

Overwrite the entire AP compact flash, destroying its contents (including the current image file). Use this command only under the supervision of Aruba technical support. If you delete the current image in the AP's flash memory, the AP will not function until you reload another image.

Parameter	Description
ap-name	Wipe out the flash of the AP with the specified name.
ip-addr	Wipe out the flash of the AP with the specified IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ap wired-ap-profile

```
ap wired-ap-profile {default | <profile-name>}
  broadcast
  clone {default | <source> }
  forward-mode {bridge|split-tunnel|tunnel}
  no
  switchport {access vlan <vlan> | mode {access|trunk} | trunk {allowed vlan <vlan-
list>| add <vlan-list> | except <vlan-list> | remove <vlan-list>}} | {native vlan
<vlan>}
  trusted
  wired-ap-enable
  wired-ap-mode {normal|daisy-chain}
```

Description

This command configures a wired AP profile. This command is only applicable to Aruba APs that support a second Ethernet port. The wired AP profile configures the second Ethernet port (enet1) on the AP.

For mesh deployments, this command is applicable to all Aruba APs configured as mesh nodes. If you are using mesh to join multiple Ethernet LANs, configure and enable bridging on the mesh point Ethernet port.

Mesh nodes only support bridge mode and tunnel mode on their wired ports (enet0 or enet1). Split tunnel mode is not supported.

Use the bridge mode to configure bridging on the mesh point Ethernet port. Use tunnel mode to configure secure jack operation on the mesh node Ethernet port.

When configuring the Ethernet ports on APs with multiple Ethernet ports, note the following requirements:

- configured as a mesh portal, connect enet0 to the managed device to obtain an IP address. The wired AP profile controls enet1. Only enet1 supports secure jack operation.
- configured as a mesh point, the same wired AP profile will control both enet0 and enet1.

Parameter	Description
ap wired-ap-profile <profile-name>	Name of this instance of the profile. The name must be 1-63 characters.
broadcast	Forward broadcast traffic to this tunnel.
clone <source>	Name of an existing wired AP profile from which parameter values are copied.

Parameter	Description
forward-mode	<p>In this default forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual. This parameter controls whether data is tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). All forwarding modes support band steering, TSPEC or TCLAS enforcement, 802.11k and station blacklisting/denylisting.</p>
bridge	<p>802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP handles all 802.11 association requests and responses, encryption or decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.</p> <p>An AP in bridge mode supports 802.1X and MAC authentication types.</p> <p>Virtual APs in bridge mode using static WEP should use key slots 2-4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.</p>
split-tunnel	<p>802.11 frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). An AP in split-tunnel mode supports only the 802.1X authentication type.</p> <p>An AP in split-tunnel forwarding mode handles all 802.11 association requests and responses, encryption or decryption, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed.</p> <p>Virtual APs in split-tunnel mode using static WEP should use key slots 2-4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.</p>
tunnel	<p>In this default forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual.</p>
no	Negates any configured parameter.
switchport	Configures the switching mode characteristics for the port.
access vlan <vlan>	The VLAN to which the port belongs. The default is VLAN 1.

Parameter	Description
<code>mode {access trunk}</code>	The mode for the port, either access or trunk mode. The default is access mode.
<code>trunk allowed vlan {add <vlan-list> except <vlan-list> remove <vlan-list> <vlan-list></code>	Allows multiple VLANs on the port interface. You must define this parameter using VLAN IDs or VLAN names. VLAN IDs and VLAN names cannot be listed together.
<code>trunk native vlan <vlan></code>	The native VLAN for the port (frames on the native VLAN are not tagged with 802.1q tags).
<code>trusted</code>	Sets port as either trusted or untrusted. The default setting is untrusted.
<code>wired-ap-enable</code>	Enables the wired AP. The wired AP is disabled by default.
<code>wired-ap-mode</code>	Enables the wired AP mode. The wired AP mode can be set to daisy-chain or normal modes.
<code>daisy-chain</code>	Enables daisy-chain mode. In this mode, the port works on trusted bridge mode and it retains the previous wired port configuration even when the controller is disconnected.
<code>normal</code>	Enables the wired AP in normal mode.

Example

The following command configures the enet1 port on a multi-port AP as a trunk port:

```
(host) [mynode] (config) #ap wired-ap-profile wiredap1
(host) [mynode] (Wired AP profile "wiredap1") #switchport mode trunk
(host) [mynode] (Wired AP profile "wiredap1") #switchport trunk allowed 4,5
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>wired-ap-mode</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode Mobility Conductor.

ap wired-port-profile

```
ap wired-port-profile {default | <profile-name>}
  aaa-profile {default | <profile-name>}
  authentication-timeout <timeout>
  auto-recovery-enable
  auto-recovery-interval <auto-recovery-interval>
  bridge-role
  broadcast-threshold <broadcast-threshold>
  clone {default | <source>}
  enet-link-profile <profile-name>
  lldp-profile {default | <profile-name>}
  loop-detection-interval <loop-detection-interval>
  loop-protect-enable
  no
  portfast
  portfast-trunk
  rap-backup
  shutdown
  spanning-tree
  storm-control-broadcast
  storm-control-broadcast-threshold
  wired-ap-profile <profile-name>
```

Description

This command configures a wired port profile. This command is only applicable to APs with Ethernet ports. Issue this command to enable or disable the wired port, define an AAA profile for wired port devices, and associate the port with an ethernet link profile that defines its speed and duplex values.

Parameter	Description
ap wired-port-profile <profile-name>	Name of this instance of the profile. The name must be 1-63 characters.
aaa-profile <profile-name>	Name of a AAA profile to be used by devices connecting to the wired port of the AP.
authentication-timeout <timeout>	Authentication timeout value, in seconds, for devices connecting the wired port of the AP. 1-65535 5

Parameter	Description
auto-recovery-enable	Enables automatic recovery of the port in the AP that is shut down because of loop protection. After the automatic recovery, if the loop re-occurs, then the port is shutdown again Disabled
auto-recovery-interval <auto-recovery-interval>	Specify the time, in seconds, to automatically recover the port in the AP that is shut down because of loop protection. 30-43200 300
bridge-role <role>	Role that is assigned to a user if split-tunnel authentication fails.
broadcast-threshold <broadcast-threshold>	Set the storm control threshold in packets per second. 1-1000000 2000
clone <source>	Create a new AP wired port profile based upon the values of an existing profile.
enet-link-profile <profile-name>	Specify an Ethernet link profile to be used by devices associated with this wired port profile. The Ethernet link profile defines the duplex value and speed to be used by the port.
lldp-profile <profile-name>	Specify an LLDP profile to be used by devices associated with this wired port profile. The LLDP profile specifies the type-length-value (TLV) elements to be sent in LLDP PDUs.
loop-detection-interval <loop-detection-interval>	Specify the time, in seconds, to send loop detection packets on the ports of an AP. 1-10 2
loop-protect-enable	Enables loop protection on the ports of an AP.

Parameter	Description
	Disabled
no	Negates any defined parameter
portfast	Enables portfast for AP wired ports. Spanning tree must be enabled before this command can be used.
portfast-trunk	Spanning tree must be enabled before this command can be used.
rap-backup	Use the <code>rap-backup</code> parameter to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the managed device. If the AP is not connected to the managed device, no firewall policies will be applied when this option is enabled. (The AAA profile will be applied when the AP is connected to managed device).
shutdown	Disable the wired AP port.
spanning-tree	Enables the spanning-tree protocol.
storm-control-broadcast	Enables the broadcast storm control. When this parameter is enabled, if the AP detects a loop on one of its Ethernet port, it shuts down the Ethernet port. This prevents the AP from receiving or sending any frames.
storm-control-broadcast-threshold	Specify the broadcast packets per second on each Ethernet port of an AP before the Ethernet port is shut down. 2000
wired-ap-profile <profile-name>	Name of a wired AP profile to be used by devices connecting the wired port of the AP. The wired AP profile defines the forwarding mode and switchport values used by the port.

Example

The following command defines a AAA profile for wired port devices:

```
(host) [mynode] (config) #ap wired-port-profile wiredport1
(host) [mynode] (AP wired port profile"wiredport1") #aaa-profile default-open
(host) [mynode] (AP wired port profile"wiredport1") #authentication-timeout
30
(host) [mynode] (AP wired port profile"wiredport1") #wired-ap-profile
wiredapl
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The following parameters were introduced: <ul style="list-style-type: none">■ auto-recovery-enable■ auto-recovery-interval■ loop-detection-interval■ loop-protect-enable■ storm-control-broadcast■ storm-control-broadcast-threshold
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ap zeroize-tpm-keys

```
ap zeroize-tpm-keys {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command is used to erase the TPM content and render an AP permanently inoperable.

Parameter	Description
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.

Example

Execute the following command to erase the TPM content and render an AP permanently inoperable.

```
(host) [mynode] (config) #ap zeroize-tpm-keys 192.168.2.4
You are about to execute a command which will make the AP inoperable and
void the RMA.
Are you sure you want to proceed? [y/n]: y
TPM keys have been zeroized. Please reboot the AP.
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable Mode.

arci-mon-log

```
arci-mon-log
enable
```

disable

Description

This command sets the status for ARCI MON debug logs.

Parameter	Description
enable	Enable ARCI MON debug logs.
disable	Disable ARCI MON debug logs.

Example

The following command enables ARCI MON debug logs.

```
(host) [mynode]arci-mon-log enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

arci-set-mon-request-timeout

```
arci-set-mon-request-timeout <time>
```

Description

This command sets MON response timeout value for webUI request.

Parameter	Description
<time>	Specify MON response timeout value in seconds for webUI request. 25 seconds

Example

The following command sets MON response timeout to 20 seconds for webUI request.

```
(host) [mynode]arci-set-mon-request-timeout 20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

arm cellular-move-sta

```
arm cellular-move-sta <mac> <est-tput>
```

Description

This command triggers a cellular handoff assist.

Parameter	Description
<mac>	MAC address of STA to kick off from wifi.
<est-tput>	Estimated throughput value(kbps).

Example

The following command triggers a cellular handoff assist.

```
(host)[mynode]arm cellular-move-sta 00:05:4e:50:14:aa 23
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

arm move-sta

```
arm move-sta <client-mac> <newbssid>
```

Description

This command moves a client station to another BSSID.

Parameter	Description
<mac>	MAC address of the client to be moved to another BSSID
<newbssid>	BSSID of the AP to which the client should associate.

Example

The following command moves a client with the MAC address **00:0B:86:01:7A:C0** to the BSSID **00:1C:B3:09:85:15**:

```
(host) [mynode] (config) #arm move-sta 00:0B:86:01:7A:C0 00:1C:B3:09:85:15
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

arp

```
arp <ipaddr> <macaddr>
```

Description

This command adds a static Address Resolution Protocol (ARP) entry. If the IP address does not belong to a valid IP subnetwork, the ARP entry is not added. If the IP interface that defines the subnetwork for the static ARP entry is deleted, you will be unable to use the arp command to overwrite the entry's current values; use the no arp command to negate the entry and then enter a new arp command.

Parameter	Description
<ipaddr>	IP address of the device to be added.
<macaddr>	Hardware address of the device to be added, in the format xx:xx:xx:xx:xx:xx.

Example

The following command configures an ARP entry:

```
(host) [node] (config) #arp 10.152.23.237 00:0B:86:01:7A:C0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

asp

```
asp login <username>
```

Description

This command is used to log in to Aruba Support Portal with a valid username and password.

Parameter	Description
<username>	Specify a username to log in to Aruba Support Portal (ASP)

Example

```
(host)[mynode]asp login default
Password:****
Please configure asp enable in asp-profile
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

audit-trail

audit-trail [all]

Description

This command enables an audit trail. By default, audit trail is enabled for all commands in configuration mode. Use the `show audit-trail` command to display the content of the audit trail.

Parameter	Description
all	Enables audit trail for all commands, including enable mode commands. The <code>audit-trail</code> command without this option enables audit trail for all commands in configuration mode.

Example

The following command enables an audit trail:

```
(host) [mynode] (config) #audit-trail
```

Related Commands

Command	Description
show audit-trail	Displays the audit trail log.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

backup

backup {config|flash}

Description

This command backs up compressed critical files in flash.

Parameter	Description
config	Backs up flash config directories to configbackup.tar.gz.
flash	Backs up flash directories to flashback.tar.gz file.

To restore these directories, use the following commands:

- `restore flash`: untar and uncompress the flashback.tar.gz file.
- `restore config`: untar and uncompress the configbackup.tar.gz file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on the Mobility Conductor.

banner

```
banner
  enforce accept
  motd <delimiter> <textString>
```

Description

This command defines a text banner to be displayed at the login prompt when a user accesses Mobility Conductor. The banner you define is displayed at the login prompt for Mobility Conductor. The banner is specific to the Mobility Conductor on which you configure it. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define, because the Mobility Conductor ends the banner when it sees the delimiter character repeated.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark (""). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.
- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Parameter	Description
<code>enforce-accept</code>	Enforces the user to accept the content added in the banner before logging in.
<code>motd</code>	Enter a message, to be displayed as a banner.
<code><delimiter></code>	Indicates the beginning and end of the banner text.
<code><textString></code>	The text you want displayed. up to 1023 characters

Example

The following example configures a banner by enclosing the text within quotation marks:


```
(host) [mynode] (config) #banner motd * "Welcome to my controller. This controller is in the production network, so please do not save configuration changes. Zach Jennings is awesome. Maintenance will be performed at 7:30 PM, so please log off before 7:00 PM."*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
(host) [mynode] (config) #banner motd *
Enter TEXT message [maximum of 1023 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '*'.

Welcome to my controller. This controller is in the production network, so please
do not save configuration changes. Zach Jennings is awesome. Maintenance will be
performed at 7:30 PM, so please log off before 7:00 PM.*
```

The banner display is as follows:

```
Welcome to my controller. This controller is in the production network, so please
do not save configuration changes. Zach Jennings is awesome. Maintenance will be
performed at 7:30 PM, so please log off before 7:00 PM.
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>enforce-accept</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

banner via

```
banner via <delimiter> <textstring>
```

Description

This command defines a login banner for Virtual Intranet Access (VIA) users. The banner you define is displayed when a user accesses VIA. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark ("). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.

- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Parameter	Description
<delimiter>	Indicates the beginning and end of the banner text.
<textstring>	The text you want displayed. up to 1023 characters

Example

The following example configures a banner by enclosing the text within quotation marks:

```
(host) [mynode] (config) #banner via * "Welcome"*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
(host) [mynode] (config) #banner via *  
Enter TEXT message [maximum of 1023 characters].  
Each line in the banner message should not exceed 255 characters.  
End with the character '*'.  
  
Welcome*
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

blmgr

```
blmgr
  trace-level
    category {all | cli | stm | syslog | utild}
      loglevel {alert | critical | debug | emergency | error | info | notice |
        warn }
```

Description

This command configures client denylist manager.

Parameter	Description
trace-level	Set parameters for debug tracing in client denylist manager.
category	Specify one of the following trace category to enable or disable: <ul style="list-style-type: none">■ all: Traces all categories■ cli: Traces in the category of CLI■ stm: Traces in the category of STM■ syslog: Traces in the category of syslog■ utild: Traces in the category of UTILD
loglevel	Specify one of the following log level of syslogs to be included in the trace: <ul style="list-style-type: none">■ alert: Trace all logs equal to or higher than LOG_ALERT.■ critical: Trace all logs equal to or higher than LOG_CRIT■ debug: Trace all logs equal to or higher than LOG_DEBUG.■ emergency: Trace all logs equal to or higher than LOG_

Parameter	Description
	EMERG. ■ error : Trace all logs equal to or higher than LOG_ERR. ■ info : Trace all logs equal to or higher than LOG_INFO . ■ notice : Trace all logs equal to or higher than LOG_NOTICE. ■ warn : Trace all logs equal to or higher than LOG_WARN .

Example

The following example enables traces in the cli category and traces all logs equal to or higher than error log.

```
(host) [mynode] (config) #blmgr trace-level category cli loglevel error
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

block-redirect-url

block-redirect-url <string>

Description

This command defines the URL to which a session is redirected if it is denied.

Parameter	Description
<string>	Redirect URL. This must be an absolute URL, with an http or https prefix.

Example

The following command configures a redirect URL. Use the `show block-redirect-url` command to view the configured redirect URLs.

```
(host) [mynode] (config) #block-redirect url https://www.redirectURL.com
```

Related Command

Command	Description
show block-redirect-url	Shows the redirect URL for blocked content.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ble_relay

```
ble_relay {export-ap-ble-all-beacon-info | export-ap-ble-ibeacon-info | send_sync_
iotcfg | set-attr <azure-log-level> <br-loglvl> <tag-logging> <ws-connect> <ws-
loglvl>}
```

Description

This command configures the Bluetooth Low Energy (BLE) relay on devices.

Parameter	Description
<code>export-ap-ble-all-beacon-info</code>	Export AP's BLE radio all Beacons parameters to a csv file.
<code>export-ap-ble-custom-beacon-info</code>	Export AP's BLE radio Custom Beacon parameters to a csv file.
<code>export-ap-ble-ibeacon-info</code>	Exports AP's BLE radio iBeacon parameters to a CSV file.
<code>send_sync_iotcfg</code>	Sends synchronized IoT configurations to the APs.
<code>set-attr</code>	Sets the attribute value.
<code>azure-log-level <azure-log-level></code>	Set one of the following azure log level for debug: <ul style="list-style-type: none">▪ none▪ error▪ info▪ trace▪ all
<code>br-loglvl <br-loglvl></code>	Process debug log for one of the following: <ul style="list-style-type: none">▪ level bitmap (AP-Transport-Profile (0x1)▪ APB Info (0x2)▪ CLI (0x4)▪ Beacon Mgmt (0x8)▪ Asset Tracking (0x10)▪ Telemetry WS (0x20)▪ Telemetry HTTPS (0x40)▪ ZF (0x80)▪ SB API(0x100)▪ WSS (0x200)▪ AZURE(0x800))
<code>tag-logging <tag-logging></code>	Initiates or terminates the tag report logging. This action is completed using binary numbers, for example 1: initiate, 0: terminate.

Parameter	Description
<code>ws-connect <ws-connect></code>	Initiates or terminates the web-socket connection. This action is completed using binary numbers, for example, 1: initiate, 0: terminate.
<code>ws-loglvl <ws-loglvl></code>	Provides the log levels to debug a web-socket connection.

Example

The following command exports the AP's BLE iBeacon information into a CSV file:

```
(host) [mynode] #ble_relay export_ap_ble_ibeacon_info
ble_info.txt file ready to be copied out
=====
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>export-ap-ble-ibeacon-info</code> parameter was introduced.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

ble_relay set-attr

```
ble_relay set-attr {azure-log-level <azure-log-level> | br-loglvl <br-loglvl> |  
tag-logging <tag-logging> | ws-connect <ws-connect> | ws-loglvl <ws-loglvl>}
```

Description

This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Parameter	Description
azure-log-level <azure-log-level>	Set one of the following azure log level for debug: <ul style="list-style-type: none">▪ none▪ error▪ info▪ trace▪ all
br-loglvl <br-loglvl>	Process debug log for one of the following: <ul style="list-style-type: none">▪ level bitmap (AP-Transport-Profile (0x1)▪ APB Info (0x2)▪ CLI (0x4)▪ Beacon Mgmt (0x8)▪ Asset Tracking (0x10)▪ Telemetry WS (0x20)▪ Telemetry HTTPS (0x40)▪ ZF (0x80)▪ SB API(0x100)▪ WSS (0x200)▪ AZURE(0x800)
tag-logging <tag-logging>	Initiates or terminates the tag report logging. Enter one of the following values: <ul style="list-style-type: none">▪ 1: initiate▪ 0: terminate
ws-connect <ws-connect>	Initiates or terminates the WebSocket connection.
ws-loglvl <ws-loglvl>	Enter the log level to debug the WebSocket connection.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

ble service-profile

```
ble service-profile <profile-name> {advertisement-format ibeacon|clone
<source>|include-ap-group <include-ap-group>|major <major-range>|minor <minor-
range>|no|radio-instance {all|external|internal}|uuid <uuid>}
```

Description

This command configures a Bluetooth Low Energy (BLE) service profile.

Parameter	Description
<profile-name>	Name of the BLE service profile.
advertisement-format ibeacon	Advertising behavior. Only iBeacon is supported.
advertisement-interval	Interval for advertised beacon. Range: [100-30000 ms] and increment in multiples of 100. Default: 500ms
clone <source>	Copy data from another BLE service profile.
custom-payload	The payload for custom beacon. The length is 3-31 bytes and each byte includes 2 ASCII characters.
include-ap-group <include-ap-group>	Applies the BLE service profile to specified AP group.
major <major-range>	Major range of iBeacon in minimum-maximum format. Default value is 0-65535.
minor <minor-range>	Minor range of iBeacon in minimum-maximum format. Default value is 0-65535.
no	Negates any configured parameter.
radio-instance	IoT radio instance to use.
all	Use all IoT radio instances.
external	Use external IoT radio instance.
internal	Use internal IoT radio instance.
uuid <uuid>	iBeacon UUID in hexadecimal format of predefined length. Example: 4152554E-F99B-4A3B-86D0-947070693A78

Example

The following command exports the AP's BLE iBeacon information into a CSV file:

```
(host) [mynode] (config) #ble service-profile default
(host) [mynode] (BLE service profile "default") #advertisement-format
ibeacon
(host) [mynode] (BLE service profile "default") #include-ap-group lobby
(host) [mynode] (BLE service profile "default") #major 0-65535
(host) [mynode] (BLE service profile "default") #minor 0-65535
(host) [mynode] (BLE service profile "default") #radio-instance all
(host) [mynode] (BLE service profile "default") #uuid 4152554E-F99B-4A3B-
86D0-947070693A78
```

Related Commands

Command	Description
show ble service-profile	Shows the BLE service profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on the Mobility Conductor.

boot

```
boot
  cf-test [fast|read-only|read-write]
  system partition <partition_id>
  verbose
```

Description

This command configures the boot options for the controller.

Parameter	Description
cf-test	Sets the type of compact flash test to run when booting the controller.
fast	Performs a fast test, which does not include media testing.
read-only	Performs a read-only media test.
read-write	Performs a read-write media test.
system partition {0 1}	Enter system partition followed by the partition number (0 or 1) that you want the controller to use during the next boot (login) of the controller. NOTE: A controller reload is required before the new boot partition takes effect.
verbose	Prints extra debugging information at boot.

Example

The following command uses system partition 1 the next time the controller boots:

```
(host) [mynode] #boot system partition 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config and Enable mode on Mobility Conductor.

branch-gateway

```
branch-gateway
  peer <IP address>
  interface vlan <vlanId>
```

Description

This command configures Branch Gateway.

Parameter	Description
<code>peer <IP address></code>	Specify IP address of transit vlan in peer gateway.
<code>interface vlan <vlanId></code>	Specify VLAN ID of the transit interface to use for sending peer traffic.

Example

The following example configures a banner by enclosing the text within quotation marks:

```
(host) [mynode] (config) #branch-gateway peer 12.3.4.5 interface vlan 2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

branch-uplink-pool

```
branch-uplink-pool <branch_pool_name> <branch_pool_start_address> <branch_pool_end_address>
```

Description

This command is used to configure branch uplink IP Pool for branch deployment. Uplink pool is configured on the VPNC's to handle duplicate IP addresses scenario on the branches.

Parameter	Description
<branch_pool_name>	Name of the pool.
<branch_pool_start_address>	Starting IP address for the pool.
<branch_pool_end_address>	Ending IP address for the pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

bulkedit import csv

```
bulkedit import csv <csv-name>
```

Description

Use the `bulkedit import csv` command to import data from a .csv file.

Parameter	Description
<code>bulkedit import csv</code>	Imports data from a .csv file.
<code><csv-name></code>	Name of the .csv file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on the managed device or the Mobility Conductor.

bulkedit export devices

bulkedit export devices

Description

Use the `bulkedit export devices` command to export data to a .csv file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on the managed device or the Mobility Conductor.

ca-bundle

```
ca-bundle
  update
    connect-timeout <timeout value>
    max-time <max-time value>
    download_url <url>
  reset
```

Description

This command upgrades/ resets the trusted CA certificates.

Parameter	Description
update	Upgrades the trusted CA certificates of managed devices.
connect-timeout<timeout value>	Time allowed, in seconds, for the managed device to connect to the server Range: 1-3600 Default: 120
max-time <max-time value>	Maximum time allowed, in seconds, for the certificates to upgrade. Range: 1-3600 Default: 120
download_url <url>	(Optional) CA certificates will be downloaded from the specified URL. If URL is not mentioned, the certificates will be downloaded from Activate. NOTE: The URL should begin with either http or https.
reset	Resets certificates to the factory default image.

Example

The following command upgrades the trusted CA certificates:

```
(host) [mynode] (config) #ca-bundle update connect-timeout 60
(host) (mynode) (config) #ca-bundle update max-time 120
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

capacity-license

```
capacity-license
enable
```

Description

This command configures capacity-license feature .

Parameter	Description
enable	Enable capacity-license feature.

Example

```
(host) [mynode] (config) #capacity-license enable
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Configure mode on Mobility Conductor.

ccm-debug

```
ccm-debug
  config-dump {disable | enable}
  config-rollback node <node-path> config-id <cfg-id>
  full-config-sync
  verify-config-sync
```

Description

Use the `ccm-debug config-rollback` command to roll back the configuration of a node to the previous version. Use this command to request a full configuration sync.

Parameter	Description
<code>config-dump</code>	Configure config dump message after write memory command. <ul style="list-style-type: none">▪ disable : Disables config dump after write memory command.▪ enable : Enables config dump after write memory command.
<code>config-rollback</code>	Rolls back to the previous configuration.
<code>node <node></code>	Specifies the configuration node.
<code>config-id <cfg-id></code>	Specifies the configuration ID (full path name of the config node) to roll back to.
<code>full-config-sync</code>	Request for a full config sync.
<code>verify-config-sync <node-path></code>	Verify if connected managed devices and Standby configurations are in sync.
<code>app-config</code>	Compare with application's running configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on the managed device or the Mobility Conductor.

cd

cd <node-path>

Description

This command changes the current configuration node to the specified node. The desired node is specified by the node-path, which can be an absolute path from the root node or relative path from the current node. Use this command to view the list of all nodes in the configuration hierarchy.

Parameter	Description
<node-path>	Path of the configuration node.

Example

The following command changes the current node-path (**/mm/mynode**) to **/md**:

```
(host) [mynode] #cd /md
(host) [md] #
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Conductor.

cfgm

```
cfgm {set config-chunk <size>|set heartbeat <time>|set timeout <time>|set  
vpnconnect_retry <retry num>}
```

Description

This command enables the configuration module on a Mobility Conductor or a managed device.

Parameter	Description
set config-chunk	Maximum packet size, in Kilobytes, that is sent every second to a managed device whenever a configuration is sent to that node. If the connection between the Mobility Conductor and managed device is slow or uneven, you can lower the size to reduce the amount of data that must be retransmitted. If the connection is very fast and stable, you can increase the size to make the transmission more efficient. 1-100 10 Kbytes
set heartbeat	Interval, in seconds, at which heartbeats are sent. You can increase the interval to reduce traffic load. 10-300 10 seconds
set timeout	Time, in seconds, of socket Rx inactivity before reconnecting with Mobility Conductor. 20-200 120 seconds
set vpnconnect_retry	VPN pre-connect packet retry heartbeat intervals . 3

Example

The following command sets the maximum packet size as 20 KB per second whenever a configuration is sent to the managed device:

```
(host) [mm] (config) #cfgm set config-chunk 20
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>set timeout</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

change-config-node

change-config-node <node-path>

Description

This command changes the current CLI node context to the specified node. The desired node is specified by the node-path, which can be an absolute path from the root node or relative path from the current node. Use this command to view the list of all nodes in the configuration hierarchy.

Parameter	Description
<node-path>	Path of the configuration node.

Example

The following command changes the current node-path (**/mm/mynode**) to **/md**:

```
(host) [mynode] #change-config-node /md
(host) [md] #
```

Related Commands

Command	Description
cd	Changes the working node to the specified path.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

clear

```
clear
aaa
acl
acl-debug
airgroup
amon-receiver
amon-sender
ap
arci-mon-mgmt-server
arp
aruba-central
ble_relay
branch-gateway-peer
counters
crypto
datapath
dds
dot1x
fault
gap-db
gsm
iap branch-key
iap statistics
iap subnet-stats
ifmap
ip
ipc
ipv6
lc-cluster [bucketmap|gsm|papi|vlan-probe]
lldp
loginsession
master-local/conductor-local
master-local-entry/conductor-local-entry
master-local-session/conductor-local-session
mon-serv
mon-serv-fwv
off-loader
openflow
openflow-controller
pan
perf-test
phonehome
port
port-security-error
process
provisioning-ap-list
provisioning-params
rap-wml
snmp
tunneled-node-mgr
```



```

ucc
update-counter
uplink
vpdn
web-cc
websocket
whitelist-db / allowlist-db
wms

```

Description

This command clears various user-configured values from your running configuration. This command clears the specified parameters of their current values.

Parameter	Description
aaa	Clear all values associated with authentication profile.
auth-survivability-cache	Clear all auth survivability cached data. Parameters: <ul style="list-style-type: none"> ▪ <code>all</code>—Clear all entries in the auth survivability cache. ▪ <code>station</code>—Clear an entry in the auth survivability cache for station.
authentication-server	Provide authentication server details to clear values specific to an authentication server or all authentication server. Parameters: <ul style="list-style-type: none"> ▪ <code>all</code>—Clear all server statistics. ▪ <code>internal</code>—Clear Internal server statistics. ▪ <code>ldap</code>—Clear LDAP server statistics. ▪ <code>radius</code>—Clear RADIUS server statistics. ▪ <code>tacacs</code>—Clear TACACS server statistics.
device-id-cache	Clear all device ID cache. Parameters: <ul style="list-style-type: none"> ▪ <code>all</code>—Clear all entries in the device ID cache.

Parameter	Description
	<ul style="list-style-type: none"> ▪ <code>mac</code>—Clear entries in the device ID cache for MAC address.
<code>load-balance statistics</code>	Clear load balance statistics. Parameters: <ul style="list-style-type: none"> ▪ <code>server group</code>—Clear load balance statistics of a server group.
<code>multiple-server-accounting statistics</code>	Clear multiple server accounting statistics. Parameters: <ul style="list-style-type: none"> ▪ <code>all</code>—Clear for all server groups. ▪ <code>server-group</code>—Clear multiple server accounting statistics for a server group.
<code>state</code>	Clear internal status of authentication modules. Parameters: <ul style="list-style-type: none"> ▪ <code>configuration</code>—Clear all configured objects. ▪ <code>debug-statistics</code>—Clear debug statistics. ▪ <code>messages</code>—Clear authentication messages that were sent and received.
<code>acl</code>	Clear ACL statistics.
<code>hits</code>	Clear ACL hit statistics.
<code>acl-debug</code>	Debug ACL hit statistics.
<code>airgroup</code>	Clear AirGroup statistics and user entries from the user table.
<code>cli-policy all</code>	Clears AirGroup policies except ClearPass Policy Manager policies.
<code>server</code>	Clears AirGroup servers.
<code>statistics</code>	<ul style="list-style-type: none"> ▪ blocked-queries—Clears the statistics of service IDs which were queried but not available in the AirGroup service table.

Parameter	Description
	<ul style="list-style-type: none"> ▪ blocked-service-id—Clears the statistics for the list of blocked services. ▪ cppm-entries—Clears the statistics that are displayed for show airgroup cppm entries command. ▪ internal-state—Clears internal state statistics of mDNS module. ▪ multi-controller—Clears the statistics maintained for multi-controller message exchanges. ▪ query—Clears statistics maintained in the user and server table. ▪ service—Clears statistics maintained in the AirGroup service table.
user	<ul style="list-style-type: none"> ▪ Mac Address—Clears the AirGroup server Mac addresses. ▪ dlna—Clears the AirGroup DLNA users. ▪ mdns—Clears the AirGroup mDNS users. ▪ all—Removes the current AirGroup user entries from the user table.
ap	Clear all AP related information.
arm bandwidth-management	Clears AP bandwidth management table counters. An AP can be specified by ap-name, BSSID, IPv4 address, or IPv6 address.
arm client-match	<ul style="list-style-type: none"> ▪ rules file-name <file-name> — Clears an imported file of ClientMatch rules. ▪ summary—Clears the ClientMatch summary information ▪ unsupported—Clears the MAC address of an unsteerable client or clients.

Parameter	Description
<pre>crash-info</pre>	Clears AP crash information. An AP can be specified by ap-name, IPv4 address, or IPv6 address.
<pre>debug</pre>	<ul style="list-style-type: none"> ▪ bss-dmo-stats— Clears DMO debug statistics from a specific BSSID of an AP. ▪ classification-counters—Clears classification counters. ▪ client-stats— Clears statistics from a client. ▪ dot11r {efficiency-stat}— Clears 802.11r-related stats. ▪ lacp—Clears transmitted and received packet counters displayed in the show ap debug lacp command. ▪ lldp—Clears LLDP for an AP. ▪ counters—Clears LLDP statistics. ▪ openflow— Clears openflow statistics. ▪ radio-stats— Clears aggregate radio debug statistics of an AP. ▪ sta-msg-stats—Clear AP-STM to STM message statistics.
<pre>mesh</pre>	Clear all mesh commands. <ul style="list-style-type: none"> ▪ debug—Clears debug information. ▪ counters—Clears statistics for a mesh node.
<pre>port {ap-name serial-num wired-mac} <port></pre>	Toggle the link on the specified port. <ul style="list-style-type: none"> ▪ ap-name—Clear specified port on AP with this name. ▪ serial-num—Clear specified port on AP with this serial number. ▪ wired-mac—Clear specified port on AP at this MAC address.
<pre>remote flash-config</pre>	Clears the flash configuration from a specified AP. An AP can be specified by ap-name, BSSID, IPv4 address, or IPv6 address.

Parameter	Description
arci-mon-mgmt-server	Clear management server counters
arm	Clear the following types of ARM ClientMatch information: <ul style="list-style-type: none"> client-match-summary client-match-unsteerable
arp	Clear all ARP table information. You can either clear all information or enter the IP address of the ARP entry to clear a specific value.
aruba-central	Clear Aruba Central WS Counters
ble_relay	Display ble relay status.
branch-gateway-peer	Display branch gateway peer information
counters	Clear all interface configuration values.
gigabitethernet	Clears configuration related to gigabitethernet ports.
port-channel <id>	Clears statistics related to a port-channel. Port-channel ID ranges from 0 to 7.
tunnel	Clears all tunnel configuration values on interface ports.
vrrp [ipv6]	Clears all VRRP configuration values on interface ports. Include the ipv6 parameter to clear IPv6 counters.
crypto	Clears the specified crypto information.
dp	Clears crypto latest DP packets.
ipsec sa [peer [[<ip-address>] [v6 <ipv6-address>]]]	Clears crypto IPsec state SAs for the following: <ul style="list-style-type: none"> peer—state for a peer v6—state for an ipv6 peer
isakmp sa [peer [[<source-ip>] [v6 <source-ipv6>]]]	Clears crypto isakmp state SAs for the following: <ul style="list-style-type: none"> peer—state for a peer v6—state for an ipv6 peer

Parameter	Description
stats	Clears crypto statistics.
datapath	<p>Clears all configuration values and statistics for the following datapath modules.</p> <ul style="list-style-type: none"> ▪ application {counters} ▪ bridge {counters} ▪ bwm {counters} ▪ compression {counters} ▪ cp-bwm {counters} ▪ crypto {counters} ▪ debug {performance} ▪ dma {counters} ▪ eap {counters} ▪ frame {counters} ▪ hardware {counters statistics} ▪ ip-fragment-table {ipv4 ipv6} ▪ ip-reassembly {counters} ▪ maintenance {counters} ▪ message-queue {counters} ▪ mobility {stats} ▪ network {egress ingress} ▪ papi {counters remote-device-table} ▪ route {counters} ▪ route-cache {A.B.C.D counters} ▪ route-cache-v6 {X:X:X:X} ▪ scheduler {counters} ▪ session {dpi counters} ▪ ssl {counters} ▪ station {counters} ▪ tcp {counters} ▪ tunnel {counters} ▪ user {counters} ▪ wan-hc {counters} ▪ web-cc {counters} ▪ wifi-reassembly {counters} ▪ wmm {counters}
dds	Clears Distributed Data Store statistics.
dot1x	<p>Clears all 802.1X-specific counters and supplicant statistics. Use the following parameters:</p> <ul style="list-style-type: none"> ▪ counters

Parameter	Description
	<ul style="list-style-type: none"> ▪ <code>supplicant-info</code>
<code>fault</code>	Clears all SNMP fault configuration.
<code>gap-db</code>	<p>Clears global AP database. This command is often used to clear all stale AP records. Use the following parameters:</p> <ul style="list-style-type: none"> ▪ <code>ap-name</code> ▪ <code>lms</code> ▪ <code>wired-mac</code> <p>To delete stale APs:</p> <ol style="list-style-type: none"> 1. Issue the <code>clear gap-db stale-ap ap-name <ap-name> lms lms-ip <lms-ip></code> command to delete a stale entry on a particular managed device. 2. Issue the <code>clear gap-db ap-name <ap-name></code> command to delete the GAP entries for the AP on the Mobility Conductor and the current LMS of the AP. <p>NOTE: The first step will delete stale entries individually from the old managed devices and the second step will remove stale entries for the Mobility Conductor and the current LMS.</p>
<code>gsm</code>	Clear GSM statistics.
<code>iap branch-key</code>	Clear IAP branch key.
<code>iap statistics</code>	Clear IAP statistics.
<code>iap subnet-stats</code>	Clear statistics of IAP subnet.
<code>ifmap</code>	Clear IF-MAP connection.
<code>ip</code>	<p>Clears IP information from DHCP bindings, IGMP groups and IP mobility configuration. Use the following parameters:</p> <ul style="list-style-type: none"> ▪ <code>dhcp</code>

Parameter	Description
	<p>Starting from ArubaOS 8.8.0.0, issue the <code>clear ip dhcp binding ip-address <ip-address></code> command to clear DHCP bindings for a specific IP address.</p> <ul style="list-style-type: none"> ▪ <code>igmp {cluster group mobility-group stats-counters}</code> ▪ <code>mobile {host multicast-vlan-table traffic trail}</code> ▪ <code>probe {stats}</code>
ipc statistics	<p>Clears all inter process communication statistics. Use the following parameters:</p> <ul style="list-style-type: none"> ▪ <code>app-ap</code> ▪ <code>app-id</code> ▪ <code>app-name</code>
app-ap	<p>Clears the statistics related to the following AP commands:</p> <ul style="list-style-type: none"> ▪ <code>am</code> ▪ <code>ofald</code> ▪ <code>sapd</code> ▪ <code>stm</code>
app-id	<p>Clears the statistics related to an application id.</p>
app-name	<p>Clears statistics application name related statistics:</p> <ul style="list-style-type: none"> ▪ aaa ▪ ads ▪ auth-resp ▪ authmgr ▪ certmgr ▪ cfgm ▪ cluster_mgr ▪ cpsec ▪ cts ▪ dbsync ▪ dds ▪ dhcp ▪ esi

Parameter	Description
	<ul style="list-style-type: none"> ▪ extifmgr ▪ fpapps ▪ gsmmgr ▪ httpd ▪ ike ▪ ip_flow_export ▪ l2tp L2TP ▪ licensemgr ▪ mdns ▪ mobileip ▪ ntp ▪ ofa ▪ ospf ▪ phonehome ▪ pim ▪ pktfilter ▪ pptp ▪ profmgr ▪ publisher ▪ resolver ▪ sapm ▪ sapm-resp ▪ snmpt ▪ stm ▪ stm-lopri ▪ syslogd ▪ ucm ▪ userdb ▪ web_cc ▪ wms
<p>ipv6</p>	<p>Clears all IPv6 session statistics, MLD group and member information, MLD statistics, counters, and DHCPv6 binding information. Use the following parameters:</p> <ul style="list-style-type: none"> ▪ <code>datapath {session}</code> ▪ <code>counters</code> ▪ <code>dhcp {binding}</code> ▪ <code>mld {cluster <stats> group proxy-mobility-group information stats-counters}</code> ▪ <code>neighbor {all ipv6}</code>

Parameter	Description
lc-cluster bucketmap publish counters	Clears the bucketmap publish counter values for the cluster on the Cluster Leader.
gsm counters	Clear GSM counter information for that cluster.
papi counters	Clear PAPI counter information for that cluster.
vlan-probe counters	Clear vlan-probe counters for that cluster.
lldp	<p>Clears LLDP information on all the interfaces. Use the following parameters:</p> <ul style="list-style-type: none"> ■ neighbors {interface gigabitethernet fastethernet slot/module/port} ■ statistics {interface gigabitethernet fastethernet slot/module/port}
loginsession	Clears login session information for a specific login session, as identified by the session id.
master-local/conductor-local	Clears all master-local/conductor-local switch statistics.
stats	<p>Clears the statistics of local or all switches connected to the Mobility Conductor or managed devices. Use the following sub-parameters:</p> <ul style="list-style-type: none"> ■ all— Clears the statistics of all the managed devices. ■ ip {ipv4-address ipv6-address}— Clears the statistics of IPv4 address or IPv6 address of the switch. ■ local-stats— Clears the master-local/conductor-local statistics at the managed device.

Parameter	Description
master-local-entry/conductor-local-entry	Clears managed device information from the Mobility Conductor LMS list. Specify the IP address of the managed device to be removed from the Mobility Conductor active LMS list.
master-local-session/conductor-local-session	Clear and reset master-local/conductor-local TCP connection. Specify the IP address of either the Mobility Conductor or managed device.
mon-serv	<p>Clears all monitoring server statistics. Use the following parameters:</p> <ul style="list-style-type: none"> ■ ap-microboot-stats — Clears the AP micro-bootstrapping statistics. ■ message-stats — Clears the monitoring and Advanced Monitoring (AMON) message statistics. ■ microboot-stats-all — Clears all micro-bootstrapping statistics. ■ radio-microboot-stats — Clears Radio micro-bootstrapping statistics. ■ sta-microboot-stats — Clears STA micro-bootstrapping statistics. ■ vap-microboot-stats — Clears VAP micro-bootstrapping statistics.
mon-serv-fw	<p>Clears all monitoring server statistics. Use the following parameters:</p> <ul style="list-style-type: none"> ■ apprf-pool-counters — Clears AppRF Pool counters. ■ message-stats — Clears the monitoring and Advanced Monitoring (AMON) message statistics.
off-loader	Clear offloader statistics.

Parameter	Description
openflow	Clear openflow statistics.
openflow-controller	Clear openflow statistics of the controller.
pan	Clear Palo Alto Networks interface.
perf-test	Clear Iperf throughput test process.
reports	Displays Iperf throughput test reports. Use the following parameters: <ul style="list-style-type: none"> ▪ ap {ap-name ip-addr ip6-addr} — All Iperf throughput test on the access point. ▪ controller — All Iperf throughput test on the controller.
phonehome	Resets phonehome stats.
port	Clear all port statistics that includes link-event counters or all counters. Use the following parameters: <ul style="list-style-type: none"> ▪ link-event ▪ stats
port-security-error gigabitethernet	Clear all port-security-error counters. Use the following parameters: <ul style="list-style-type: none"> ▪ slot ▪ module ▪ port
process	Clear Process level operations.
fpapps	Clear information from Level7's Layer2/Layer3 module.
message-queue-stats	Clear statistics on Fpapps internal message queue operations.
task-stats	Clear statistics on Fpapps internal OS API tasks.
timer-stats	Clear statistics on Fpapps Internal Timer Module.

Parameter	Description
<code>provisioning-ap-list</code>	Clear APs from provisioning list.
<code>provisioning-params</code>	Clear provisioning parameters and reset them to the default configuration values.
<code>rap-wml</code>	Clear wired MAC lookup cache for a DB server.
<code>snmp</code>	Clear SNMP information.
<code>tunneled-node-mgr</code>	Clear tunneled node manager information.
<code>ucc</code>	Clear UCC state information.
<code>client ip <ipaddr></code>	Clear the UCC counter for a client.
<code>sessions ip <ipaddr></code>	Clear active UCC sessions based on a specific client IP address.
<code>statistics counter call {client global}</code>	Clear UCC call statistics based on particular client or system wide.
<code>update-counter</code>	Clear all update counter statistics.
<code>uplink</code>	Clear uplink manager configuration.
<code>vpdn</code>	Clear all VPDN configuration for L2TP and PPTP tunnel. Use the following parameters: <ul style="list-style-type: none"> ■ <code>tunnel l2tp id <l2tp-tunnel-id></code> ■ <code>tunnel pptp id <pptp-tunnel-id></code>
<code>web-cc</code>	Clear all web content classification information.
<code>web-cc cache <MD5-1></code>	Clear web content category URLs from the datapath cache by specifying the two MD5 values of the URL to be removed from the cache. To view all entries in the datapath, and the MD5 values for each entry, issue the command <code>show datapath web-cc</code> .

Parameter	Description
<code>web-cc stats</code>	Clear all web content classification statistics. To view current statistics information, issue the command <code>show web-cc stats</code> .
<code>web-cc md</code>	Clear all web content classification managed nodes. Use the following parameter: <ul style="list-style-type: none"> ▪ <code>stats</code> — Clears all web content classification statistics.
<code>websocket</code>	Clear Web-Socket Interface statistics.
<code>whitelist-db/ allowlist-db</code>	Clear whitelist/allowlist statistics. Use the following parameter: <ul style="list-style-type: none"> ▪ <code>cpsec-stats</code> — Clear CPsec whitelist/allowlist statistics.
<code>wms</code>	Clear all WLAN management commands. Use the following parameters: <ul style="list-style-type: none"> ▪ <code>ap</code> — All AP related commands. Specify the BSSID of the AP. ▪ <code>client</code> — Clear all wired client related commands. Specify the MAC address of the client. ▪ <code>event</code> — Clears all events. Parameters: <ul style="list-style-type: none"> ▪ <code>database-id</code> — Clear a single event with database id. ▪ <code>event-type</code> — Clear all events with type. ▪ <code>target-mac</code> — Clear all events assigned to a target MAC. ▪ <code>probe</code> — Clear all probe information. Specify the BSSID of the probe.
<code>ap</code>	Clear AP information.
<code>client</code>	Clear client information.
<code>event</code>	Clear event information.
<code>probe</code>	Clear probe information.

Parameter	Description
wired-mac	<p>Clear learned and collected wired-mac information:</p> <ul style="list-style-type: none"> ▪ all — Clear all learned and collected wired mac information. ▪ gw-mac — Clear gateway wired mac information collected from APs. ▪ monitored-ap-wm — Clear monitored AP wired mac information collected from APs. ▪ prop-eth-mac — Clear wired mac information collected from APs. ▪ reg-ap-oui — Clear registered AP OUI information collected from APs. ▪ system-gw-mac — Clear system gateway mac information learned at the controller . ▪ system-wired-mac — Clear system wired mac information learned at the controller. ▪ wireless-device — Clear routers or potential wireless devices information.

Example

The following command clears all aaa counters for all authentication servers:

```
(host) [mynode] #clear aaa authentication-server all
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The <code>clear lc-cluster bucketmap publish counters</code> command was introduced.
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .

Release	Modification
	All instances of <code>master-local-entry</code> have been replaced with <code>conductor-local-entry</code> . All instances of <code>master-local-session</code> have been replaced with <code>conductor-local-session</code> .
ArubaOS 8.8.0.0	The <code>ip dhcp binding ip-address <ip-address></code> parameter was introduced.
ArubaOS 8.6.0.17 and 8.7.1.9	The iap statistics , iap branch-key , and iap subnet-stats parameters were introduced.
ArubaOS 8.6.0.0	The <code>route-cache-v6</code> sub-parameter was added to the <code>datapath</code> parameter.
ArubaOS 8.3.0.0	The <code><port></code> sub-parameter was added to the <code>port</code> parameter.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>master-local</code> ■ <code>mon-serv</code> ■ <code>mon-serv-fwv</code> ■ <code>perf-test</code> ■ <code>web-cc md</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

clear amon-receiver

```
show amon-receiver [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-  
stats-inst-1] | [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] |  
[dest-stats-inst-5] | [dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] |  
[error-counters] | [error-counters-all] | [interest-table] | [list-details] |  
[parameter] | [set-debug-level-dest] | [src-stats-all] | [stats-counters] | [stats-  
counters-all]]
```

Description

This command displays AMON receiver information.

Parameter	Description
dest-stats-all	Clear all destination statistics
dest-stats-inst-0	Clears destination statistics instance 0
dest-stats-inst-1	Clears destination statistics instance 1
dest-stats-inst-2	Clears destination statistics instance 2
dest-stats-inst-3	Clears destination statistics instance 3
dest-stats-inst-4	Clears destination statistics instance 4
dest-stats-inst-5	Clears destination statistics instance 5
dest-stats-inst-6	Clears destination statistics instance 6
dest-stats-inst-7	Clears destination statistics instance 7
error-counters	Clears error counters
src-stats-counters	Clears stats counters for a particular source
src-stats-counters-all	Clears all stats counters for all sources
stats-counters	Clears stats counters
stats-counters-all	Clears all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] #clear amon-receiver dest-stats-inst-0
```

```
Clear Amon Receiver Stats
-----
AMON-RECEIVER
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

clear amon-sender

```
show amon-sender [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-  
stats-inst-1] | [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] |  
[dest-stats-inst-5] | [dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] |  
[error-counters] | [error-counters-all] | [interest-table] | [list-details] |  
[parameter] | [set-debug-level-dest] | [src-stats-all] | [stats-counters] | [stats-  
counters-all]]
```

Description

This command displays AMON sender information. This command must be issued on the managed device.

Parameter	Description
bundle-counters	Clears bundle counters
dest-stats-inst-0	Clears destination statistics instance 0.
dest-stats-inst-1	Clears destination statistics instance 1.
dest-stats-inst-2	Clears destination statistics instance 2.
dest-stats-inst-3	Clears destination statistics instance 3.
dest-stats-inst-4	Clears destination statistics instance 4.
dest-stats-inst-5	Clears destination statistics instance 5.
dest-stats-inst-6	Clears destination statistics instance 6.
dest-stats-inst-7	Clears destination statistics instance 7.
egress-counters	Clears egress counters.
error-counters	Clears error counters.
src-stats-counters	Clears stats counters for a particular source.
src-stats-counters-all	Clears stats counters for all sources.
stats-counters	Clears stats counters.
stats-counters-all	Clears all stats counters.

Example

The following command displays AMON sender information for destination statistics instance 0:

```
(host) [mynode] #logon 192.0.1.12
(MN-7240) #clear amon-sender dest-stats-inst-0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

clear wms wired-mac

```
clear wms wired-mac [ all | gw-mac <mac> | monitored-ap-wm <mac> | prop-eth-mac <mac> | reg-ap-oui <mac> | system-gw-mac <mac> | system-wired-mac <mac> | wireless-device <mac>]
```

Description

Clear *learned* and *collected* Wired MAC information. Optionally, enter the MAC address, in **nn:nn:nn:nn:nn:nn** format, of the AP that has seen the Wired MAC.

Parameter	Description
all	Clear all the learned and collected wired Mac information.
gw-mac <mac>	Clear the gateway wired Mac information collected from the APs.
monitored-ap-wm <mac>	Clear monitored AP wired Mac information collected from the APs.
prop-eth-mac <mac>	Clear the wired Mac information collected from the APs.
reg-ap-oui <mac>	Clear the registered AP OUI information collected from the APs.
system-gw-mac <mac>	Clear system gateway Mac information learned at the controller.
system-wired-mac <mac>	Clear system wired Mac information learned at the controller.
wireless-device <mac>]	Clear routers or potential wireless devices information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config and Enable mode on Mobility Conductor.

clock cli-timestamp

clock cli-timestamp

Description

This command enables the timestamp feature, adding a date and time to the output of `show` commands.

When you enable the timestamp feature, the CLI includes a timestamp in the output of each `show` command indicating when the `show` command was issued. Note that the output of `show clock` and `show log` commands do not include timestamps, even when this feature is enabled. You can disable timestamps using the command `no clock cli-timestamp`.

Example

The following example enables the timestamp feature.

```
(host) [mynode] (config) #clock cli-timestamp
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

clock set

```
clock set <year> <month> <day> <time>
```

Description

This command sets the date and time. You can configure the year, month, day, and time. You must configure all four parameters.

Specify the time using a 24-hour clock. You must specify the seconds.

Parameter	Description
clock set	Sets the time and date.
<year>	Sets the year. Requires all 4 digits. Numeric
<month>	Sets the month. Give the complete month name. january-december
<day>	Sets the day. 1-31
<time>	Sets the time. Specify hours, minutes, and seconds separated by spaces. 0-23 for hours 1-60 for minutes 1-60 for seconds

Example

The following example configures the clock to January 1, 2017, at 16:22:52.

```
(host)[mynode] #clock set 2017 january 1 16 22 52
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode or Config mode on Mobility Conductor.

clock summer-time recurring

```
clock summer-time <WORD> recurring  
  <1-4> <start day> <start month> <hh:mm>  
  first <start day> <start month> <hh:mm>  
  last <start day> <start month> <hh:mm>  
  <1-4> <end day> <end month> <hh:mm>  
  first <end day> <end month> <hh:mm>  
  last <end day> <end month> <hh:mm>
```

Description

This command sets the software clock to begin and end daylight savings time on a recurring basis. This command subtracts exactly 1 hour from the configured time.

The **WORD** can be any alphanumeric string, but cannot start with a colon (:). A **WORD** longer than five characters is not accepted. If you enter a **WORD** containing punctuations, the command is accepted, but the timezone is set to UTC.

You can configure the time to change on a recurring basis. To do so, set the week, day, month, and time when the change takes effect (daylight savings time starts). You must also set the week, day, month, and time when the time changes back (daylight savings time ends).

The **start day** requires the first three letters of the day. The **start month** requires the first three letters of the month.

You also have the option to set the number of hours by which to offset the clock from UTC. This has the same effect as the [clock timezone](#) command.

Parameter	Description
<WORD>	Abbreviation for your time zone. For example, PDT for Pacific Daylight Time. 3-5 characters
<1-4>	Enter the week number to start and end daylight savings time. For example, enter 2 to start daylight savings time on the second week of the month. 1-4
first	Enter the keyword first to have the time change begin or end on the first week of the month.
last	Enter the keyword last to have the time change begin or end on the last week of the month.
<start day>	Enter the weekday when the time change begins or ends. Sunday-Saturday
<start month>	Enter the month when the time change begins or ends.

Parameter	Description
	January-December
<hh:mm>	Enter the time, in hours and minutes, that the time change begins or ends. 24 hours

Example

The following example sets daylight savings time to occur starting at 2:00 AM on Sunday in the second week of March, and ending at 2:00 AM on Sunday in the first week of November. The example also sets the name of the time zone to PST with an offset of UTC - 8 hours.

```
(host) [mynode] (config) #clock summer-time PST recurring 2 Sun Mar 2:00
first Sun Nov 3:00 -8
```

Related Commands

Command	Description
show clock	Displays the system clock, configured for daylight savings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

clock timezone

clock timezone <name>

Description

This command sets the timezone on a controller. The `name` parameter can be any alphanumeric string, but cannot start with a colon (:). A time zone name longer than five characters is not accepted. If you enter a time zone name containing punctuation, the command is accepted, but the time zone is set to UTC.

Parameter	Description
<name>	Name of the timezone. 3-5 characters

Example

The following example configures the timezone to PST.

```
(host) [mynode] (config) #clock timezone PST
```

Related Commands

Command	Description
show clock	Displays the system clock under the configured timezone.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

clear aaa auth-survivability-cache

clear aaa auth-survivability-cache

Description

This command allows you to clear the data that is currently in the local Survival Server cache.

Parameter	Description
all	Clears all entries in the Authentication Survivability Cache.
station	Clears the entry in the Authentication Survivability Cache for a particular station.
A:B:C:D:E:F	Specify the MAC address of the station.

Example

To clear the auth-survivability cache:

```
(host) [mynode] (config) #clear aaa auth-survivability-cache <all> |  
<station MAC_address>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

cluster-debug

cluster-debug

```
bucketmap {rebalance | essid <ssid_name> {bucketindex <buck_idx>| active
<active_uac_idx> | standby <standby_uac_idx>}}
standby-aac reassign [[active-aac-ip] <active_aac> [active-aac-ip6]] <active_aac_
v6> [[standby-aac-ip] [standby-aac-ip6]] <new_standby_aac> <new_standby_aac_v6>
[ap-group] <ap-group> [ap-mac] <ap-mac>
calc-sta-uac <sta_mac> <ssid_name>
```

Description

This command set is used to change the bucketmap entries and to reassign the standby AAC. However, changing the bucketmap entries is not recommended by Aruba.

Parameter	Description
bucketmap	Bucket map.
rebalance	Evenly rebalance bucketmap distribution based on the cluster node's platform capacity. NOTE: The cluster-debug bucketmap rebalance command is disruptive and disconnects all the connected clients. To minimize impact on clients, run this command with caution, possibly during a maintenance window.
ssid <ssid_name>	Essid name.
Bucketindex <0-255>	Index within bucket map. The valid range of values for index is <0-255>.
active <0-11>	Index of UAC in bucket map's UAC List. The valid range of values for index is <0-11>.
standby <standby_uac_idx>	Standby UAC . Index of UAC in bucket map's UAC List or -1 if no standby desired. The valid range of values for index is <0-11>.
calc-sta-uac	Calculate station UAC and index by using bucketmap in GSM channel.
<sta_mac>	Enter the station MAC Address.
<ssid_name>	Enter the Essid name.
standby-aac	Standby AAC.
reassign	Reassign Standby AAC.

Parameter	Description
active-aac-ip <active_aac>	Active AAC IP Address. Enter the IP address of Active AAC. Use the following parameters: <ul style="list-style-type: none"> standby-aac-ip <new_standby_aac>: Enter the IP Address of new standby AAC. standby-aac-ip6 <new_standby_aac_v6>: Enter the IPv6 Address of new standby AAC.
active-aac-ip6 <active_aac_v6>	Active AAC IPv6 Address. Enter the IPv6 address of Active AAC.
ap-group <ap-group>	Enter the AP Group name. Use the following parameters: <ul style="list-style-type: none"> active-aac-ip <active_aac>: Enter the IP Address of active AAC. active-aac-ip6 <active_aac_v6>: Enter the IPv6 Address of active AAC. standby-aac-ip <new_standby_aac>: Enter the IP Address of new standby AAC. standby-aac-ip6 <new_standby_aac_v6>: Enter the IPv6 Address of new standby AAC.
ap-mac <ap_mac>	Enter the AP MAC Address.

Command History

Release	Modification
ArubaOS 8.6.0.17 and 8.7.1.9	The bucketmap rebalance parameter was introduced.
ArubaOS 8.2.0.0	The <code>calc-sta-uac</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

cluster-member-custom-cert

```
cluster-member-custom-cert member-mac <mac> ca-cert <ca> server-cert <cert>  
suite-b <gcm-128 | gcm-256>]
```

Description

This command sets the managed device as a CPsec cluster root, and specifies a custom user-installed certificate for authenticating cluster members. If your network includes multiple Mobility Conductor each with their own hierarchy of APs and managed device, you can allow APs from one hierarchy to failover to any other hierarchy by defining a cluster of Mobility Conductor. Each cluster will have one Mobility Conductor as its cluster root, and all other managed devices as cluster members.

To define a managed device as a cluster root, issue one of the following commands on that managed device:

- [cluster-member-custom-cert](#): Define the Mobility Conductor as a cluster root, and select a user-installed certificate to authenticate that cluster member.
- [cluster-member-factory-cert](#): Define the Mobility Conductor as a cluster root, and select a factory-installed certificate to authenticate that cluster member.
- [cluster-member-ip](#) : Define the Mobility Conductor as a cluster root, and set the IPsec key to authenticate that cluster member.



For information on installing certificates on your controller, refer to the *Management Utilities* chapter of the *ArubaOS User Guide*.

Parameter	Description
member-mac <ca>	MAC address of the cluster member.
ca-cert <ca>	Name of the CA certificate uploaded via the WebUI.
ca-cert <ca>	Name of the CA certificate uploaded via the WebUI.
server-cert <cert>	Name of the server certificate uploaded via the WebUI.
suite-b	To use Suite-B encryption in the secure communication between the cluster root and cluster member, specify one of the following Suite-B algorithms: <ul style="list-style-type: none">▪ gcm-128: Encryption using 128-bit AES-GCM▪ gcm-256: Encryption using 256-bit AES-GCM

Example

The following example selects a customer installed certificate for cluster member authentication.

```
(host) (config) # cluster-member-custom-cert member-mac 00:1E:37:CB:D4:52 ca-  
cert cacert1 server-cert servercert1
```

Related Commands

Parameter	Description
control-plane-security	Configure the CPsec profile.
show cluster-config	Show the multi-master/conductor cluster configuration for the CPsec feature.
show cluster-switches	Issue this command on a Mobility Conductor using CPsec in a multi-master/conductor environment to show other managed devices to which it is connected.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

cluster-member-factory-cert

cluster-member-factory-cert member-mac <mac>

Description

This command sets the managed device as a CPsec cluster root, and specifies a custom user-installed certificate for authenticating cluster members. To define a controller as a cluster root, issue one of the following commands on that controller:

- [cluster-member-custom-cert](#): Define the managed device as a cluster root, and select a user-installed certificate to authenticate that cluster member.
- [cluster-member-factory-cert](#): Define the managed device as a cluster root, and select a factory-installed certificate to authenticate that cluster member.
- [cluster-member-ip](#): Define the Managed device as a cluster root, and set the IPsec key to authenticate that cluster member.



For information on installing certificates on your controller, refer to the *Management Utilities* chapter of the *ArubaOS User Guide*.

Parameter	Description
<mac>	MAC address of the user-installed certificate on the cluster member.

Example

The following command sets the managed device on which you issue command as a root managed device, and adds the managed device **172.21.18.18** as a cluster member with the IPsec key **ipseckey1**:

```
(host) (config) #cluster-member-factory-cert member-mac 00:1E:37:CB:D4:52
```

Related Commands

Parameter	Description
control-plane-security	Configure the CPsec profile.

Parameter	Description
<u>show cluster-config</u>	Show the multi-master/conductor cluster configuration for the CPsec feature.
<u>show cluster-switches</u>	Issue this command on a Mobility Conductor using CPsec in a multi-master environment to show other managed devices to which it is connected.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

cluster-member-ip

```
cluster-member-ip <ip-address>  
    ipsec <key>
```

Description

This command sets the Mobility Conductor as a CPsec cluster root, and specifies the IPsec key for a cluster member. The Mobility Conductor operating as the cluster root will use the CPsec feature to create a self-signed certificate, then certify its own managed devices and APs. Next, the cluster root will send the certificate to each cluster member, which in turn certifies their own managed devices and APs. Since all managed devices and APs in the cluster get their certificates from the cluster root, they will all have the same trust anchor, and the APs can switch to any other managed device in the cluster and still remain connected to the secure network.

Issue the [cluster-member-ip](#) command on the Mobility Conductor you want to define as the cluster root to set the IPsec key for secure communication between the cluster root and each cluster member. Use the IP address **0.0.0.0** in this command to set a single IPsec key for all member managed devices, or repeat this command as desired to define a different IPsec key for each cluster member.

Once the cluster root has defined an IPsec key for all cluster members, you must access each of the member managed devices and issue the command [cluster-root-ip](#) to define the IPsec key for communication to the cluster root.

Parameter	Description
<ip-address>	Switch IP address of a CPsec cluster member. You can also use the IP address 0.0.0.0 to set a single IPsec key for all cluster members.
ipsec <key>	Configure the value of the IPsec key for secure communication between the cluster root and the specified cluster member. The key must be between 6-64 characters.

Example

The following command sets the managed device on which you issue command as a root managed device, and adds the managed device **172.21.18.18** as a cluster member with the IPsec key **ipseckey1**:

```
(host) (config) #cluster-member-ip 172.21.18.18 ipsec ipseckey1
```

Related Commands

Parameter	Description
control-plane-security	Configure the CPsec profile.
show cluster-config	Show the multi-master/conductor cluster configuration for the CPsec feature.
show cluster-switches	Issue this command on a Mobility Conductor using CPsec in a multi-master environment to show other managed devices to which it is connected.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

cluster-root-ip

```
cluster-root-ip <ip-address>  
  ipsec <key>  
  ipsec-custom-cert root-mac1 <mac1> [root-mac2 <mac2>] ca-cert <ca> server-cert  
  <cert> [suite-b <gcm-128 | gcm-256>]  
  ipsec-factory-cert root-mac-1 <mac> [root-mac-1 <mac>]
```

Description

This command sets the Mobility Conductor as a CPsec cluster member, and defines the IPsec key or certificate for secure communication between the cluster member and the Mobility Conductor's cluster root.

Parameter	Description
<ip-address>	The IP address of CPsec cluster root Mobility Conductor. To set a single IPsec key for all member managed devices in the cluster, use the IP address 0.0.0.0 .
ipsec <key>	Set the value of the IPsec PSK for communication with the cluster root. This parameter must be have the same value as the IPsec key defined for the cluster member via the cluster-member-ip command.
ipsec-factory-cert	Use a factory-installed certificate for secure communication between the cluster root and the specified cluster member by specifying the MAC address of the certificate.
root-mac-1 <mac>	Specify MAC address of the cluster root.
ipsec-custom-cert	Use a custom user-installed certificate for secure communication between the cluster root and the specified cluster member.
root-mac-1 <mac>	Specify the MAC address of the cluster-root's certificate.
root-mac-2 <mac>	(Optional) If your network has multiple Mobility Conductor, use this parameter to specify he MAC address of the redundant cluster-root's certificate.
ca-cert <ca>	Name of the CA certificate uploaded via the WebUI
server-cert <cert>	Name of the server certificate uploaded via the WebUI.
suite-b	To use Suite-B encryption in the secure communication between the cluster root and cluster member, specify one of the following Suite-B algorithms <ul style="list-style-type: none">▪ gcm-128: Encryption using 128-bit AES-GCM▪ gcm-256: Encryption using 256-but AES-GCM

Example

The following command defines the IPsec key for communication between the cluster member and the root managed device **172.21.45.22**:

```
(host) [mynode] (config) #cluster-root-ip 172.21.45.22 ipsec ipseckey1
```

Related Commands

Parameter	Description
control-plane-security	Configure the CPsec profile.
show cluster-config	Show the multi-master/conductor cluster configuration for the CPsec feature.
show cluster-switches	Issue this command on a Mobility Conductor using CPsec in a multi-master environment to show other managed devices to which it is connected.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

cm_mu_client_thresh

cm-mu-client-thresh <count>

Description

This ClientMatch command configures the client threshold on a multi-user-capable (MU-capable) radio. This command is used when MU-capable clients attempt to steer to a MU-capable radio. Clients are not steered to radios that have already met the client threshold, preventing the need for load-balancing.

Parameter	Description
count	Total number of clients that can be associated to a radio, in which the radio can still be considered for MU-steering. 15

Example

The following example configures a threshold of 12 clients on a MU-MIMO-capable radio:

```
(host) (config) #cm-mu-client-thresh <12>
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

cm_mu_snr_thresh

cm-mu-snr-thresh <value>

Description

This ClientMatch command configures the Signal to Noise Ratio (SNR) threshold for a multi-user-capable (MU-capable) radio. The **cm-mu-snr-thresh** value must be greater than the **cm-sticky-snr** value for a MU-capable client to be steered to that radio.

Parameter	Description
value <dB>	Minimum SNR value of a client on the target radio, in which the radio can still be considered for MU-steering. > 25 30

Example

The following example configures an SNR threshold of 90 on a MU-MIMO-capable radio:

```
(host) (config) #cm-mu-snr-thresh <90>
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

command-set-profile

command-set-profile <profile-name>

Description

This command configures a command set profile.

Parameter	Description
<profile-name>	Specify name of the profile to configure.

Example

```
(host) [mynode] (config) #command-set-profile default
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Configure mode on Mobility Conductor.

controller-amon

```
controller-amon  
  bssid-tunnel-stats
```

Description

This command configures controller AMON process.

Parameter	Description
bssid-tunnel-stats	Enable sending cluster statistics in AMON feed.

Example

```
(host) [mynode] (config) #controller-amon bssid-tunnel-stats
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Configure mode on Mobility Conductor.

controller-ble

```
controller-ble  
  opmode { disabled| PersistentConsole}
```

Description

This command displays controller information.

Parameter	Description
opmode	Configure one of the following BLE operational mode for 90xx series controllers: <ul style="list-style-type: none">■ disabled: BLE is turned off.■ PersistentConsole: BLE radio allows serial console access over BLE alongwith beaconing.

Example

```
(host) [mynode] (config) #controller-ble opmode PersistentConsole
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Configure mode on Mobility Conductor.

controller-ble opmode

```
disabled  
persistentconsole
```

Description

This command configures the BLE operation mode of a controller.

Parameter	Description
disabled	In the disabled opmode, the BLE radio in a controller is turned off. Disabled
persistentconsole	In the persistentconsole opmode, the BLE radio in a controller allows serial console access over BLE along with beaconing.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>beaconing</code> parameter was removed.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

control-plane-security

```
control-plane-security
  auto-cert-allow-all
  auto-cert-allowed-addr <start> <end>
  auto-cert-allowed-addr <startv6> <endv6>
  auto-cert-prov
  cpsec-enable
  no
  timer
```

Description

Configure the control plane security profile by identifying APs to receive security certificates.

The managed devices enabled with control plane security only send certificates to APs that you have identified as valid APs on the network. If you are confident that all campus APs currently on your network are valid APs, you can configure automatic certificate provisioning to send certificates from the managed device to each campus AP, or to all campus APs within a specific range of IP addresses. If you want closer control over each AP that gets certified, you can manually add individual campus APs to the secure network by adding each AP's information to a campus AP whitelist/allowlist.

Parameter	Description
<code>auto-cert-allow-all</code>	When you issue the control-plane-security auto-cert-allow-all command, the managed device sends a certificate to all associated APs when auto certificate provisioning is enabled. When disabled, the managed device sends certificates only to APs whose IP or IPv6 addresses are in the ranges specified by auto-cert-allowed-addr .
<code>auto-cert-allowed-addr <start> <end></code>	Use this command to define a specific range of AP IP addresses. The managed device sends certificates to the APs in this IP range when auto certificate provisioning is enabled. Identify a range by entering the starting IP address and the ending IP address in the range, separated by a single space. You can repeat this command as many times as necessary to define multiple IP ranges.
<code>auto-cert-allowed-addr <startv6> <endv6></code>	Use this command to define a specific range of AP IPv6 addresses. The managed device sends certificates to the APs in this IPv6 range when auto certificate provisioning is enabled. Identify a range by entering the starting IPv6 address and the ending IPv6 address in the range, separated by a single space. You can repeat this command as many times as necessary to define multiple IP ranges.

Parameter	Description
<code>auto-cert-prov</code>	Issue this command to enable automatic certificate provisioning. When this feature is enabled, the managed device will attempt to send certificates to associated APs. To disable this feature, use the command <code>no auto-cert-prov</code> . Automatic certificate provisioning is disabled by default
<code>cpsec-enable</code>	Issue this command to enable control plane security. To disable this feature, use the command <code>no cpsec-enable</code> . Control plane security is enabled by default.
<code>no</code>	Negates any configured parameter.
<code>timer <timer></code>	Timer value, in dd:hh (days:hours) format, that prevents APs from going into unapproved-no-cert state when the APs remain idle for two or more hours. The minimum value of hours in dd:hh format is 2 hours.

Example

The following command defines a range of IP addresses that should receive certificates from the managed device, and enables the control plane security feature:

```
(host) [md] (config) #control-plane-security
auto-cert-allowed-addr 10.21.18.10 10.21.10.90
cpsec-enable
```

Related Commands

Command	Description
show control-plane-security	Displays the configured control plane security profile settings.

Command History

Release	Modification
ArubaOS 8.3.0.0	The <code>timer</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

configuration device

```
configuration device
  default-node <node-path>
  file <mac address>
  <mac-address> device-model
  {A7005|A7008|A7010|A7024|A7030|A7205|A7210|A7220|A7240|A7240XM|A7280|MC-VA}
  [<config-path>] |move-to[<dest-path>] [<mac-address-2>]
```

Description

This command maps a device to an existing node in the configuration hierarchy.

The node to which the device is mapped is specified by the `node-path`, which can be an absolute path from the root node or relative path from the current node. If the `node-path` is not specified, the device is mapped to the current node. A device-specific node is created to store the configuration for the device. The node is named using the specified MAC address of the device.

Use the `show configuration devices` command to view the complete list of devices provisioned on your Mobility Conductor, and the `show configuration node-hierarchy` command to view the list of all nodes in the configuration hierarchy.

Parameter	Description
<code>default-node <node-path></code>	Specifies the node to which any device without explicit device-node mapping is attached. If a default node is not configured, unknown devices cannot connect to Mobility Conductor.
<code>file</code>	Use file for initially configuring the node
<code><mac-address></code>	MAC address of the device to be added.
<code><mac-address></code>	MAC address of a device that must be mapped to a node in the configuration hierarchy.
<code>device-model</code>	Model number for the device: <ul style="list-style-type: none">▪ A7005▪ A7008▪ A7010▪ A7024▪ A7030▪ A7205▪ A7210▪ A7220▪ A7240▪ A7240XM▪ A7280▪ MC-VA

Parameter	Description
<config-path>	Full configuration path to which the device is mapped. If the path is not specified, the device is mapped to the current node.
move-to <dest-path>	Moves the device to the specified configuration path of the destination node.
<mac-address-2>	MAC address of the destination node in the configuration hierarchy.

Example

The following command specifies **/md** as the default node:

```
(host) [mynode] (config) #configuration device default-node /md
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The <code>A7280</code> option was added under the <code>device-model</code> parameter.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>move-to</code> ■ <code>dest-path</code> ■ <code>mac-address-2</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

configuration node

```
configuration node
  replace-config <filename> [ignore-masterip-config] [<node-path>]
  replace-config-reboot
  <node-path>
    clone-from <source-path>
    file config-file <filename>
    move-to <dest-path>
```

Description

This command configures nodes in the configuration hierarchy. Node name and location are specified by the node-path, which can be an absolute path from the root node or relative path from the current node. Use this command to view the list of all nodes in the configuration hierarchy.

Parameter	Description
replace-config <filename>	New configuration file to be applied for the specified node.
ignore-masterip-config	(Optional) Ignores any master/conductor IP related changes from the specified configuration file.
<node-path>	(Optional) Path of the configuration node to which the new configuration is to be applied.
replace-config-reboot <filename1>	Replace node's configuration with the configuration file name provided and then reboot.
<node-path>	Path of the configuration node to be added, removed, or moved.
clone-from <source-path>	Copies an existing node's configuration to a new node. The source and destination node names and locations are specified by the source node-path and node-path, respectively.
file config-file <filename>	Use configuration file for initially configuring the node.
move-to <dest-path>	Moves an existing user-created node in the hierarchy to the specified destination node. System-generated nodes cannot be moved. Ensure the following points while moving a node or device, otherwise the move operation will fail: <ul style="list-style-type: none">▪ The node to be moved is a leaf node and does not have any group node or a device node as a child node under it.▪ No configuration is pending on the parent nodes of the child node to be moved.▪ The configuration on the node to be moved is compliant with the configuration in the new ancestor nodes chain.

Example

The following command clones the **/md/group2** node-path to the **/md/group1** node:

```
(host) [mynode] (config) #configuration node /md/group1 clone-from /md/group2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>move-to</code> sub-parameter was introduced under the <code><node-path></code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

configuration purge-pending-config

configuration purge-pending-config [<node-path>]

Description

This command cleans up any pending configurations on nodes in the configuration hierarchy. Issue this command without the <node-path> parameter to purge all pending configurations in the hierarchy. Use the `show configuration node-hierarchy` command to view the list of all nodes in the configuration hierarchy.

Parameter	Description
<node-path>	Path of the configuration node to be purged.

Example

The following command cleans up pending configuration on the **/md** node:

```
(host) [mynode] (config) #configuration purge-pending-config /md
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

configuration rename

```
configuration rename  
  <old-path>  
  <new-path>
```

Description

This command renames a node path to the specified new name.

Parameter	Description
<old-path>	Name and path of the node to be renamed.
<new-path>	Renames the existing node name to the specified name. The node paths of the child nodes under the renamed node are automatically updated.

Example

The following command renames the **/md/node1** node-path to the **/md/node2** node:

```
(host) [mynode] (config) #configuration rename /md/node1 /md/node2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

configure terminal

```
configure terminal
  ids unauthorized-device-profile <profile name>
    detect-wifi-direct-p2p-groups | wifi-direct-network-quiet-time | protect-wifi-
    direct-p2p-groups
```

Description

This command allows you to enter the configuration mode. Starting from ArubaOS 8.11.0.0, this command allows you to configure the Wi-Fi Direct settings of an **IDS Unauthorized Device** profile.

Parameter	Description
<code>ids unauthorized-device-profile <profile name></code>	Name of the IDS Unauthorized Device profile.
<code>detect-wifi-direct-p2p-groups</code>	Indicates if the Wi-Fi Direct detection is turned on or off.
<code>wifi-direct-network-quiet-time</code>	The wait time, in seconds, after detecting a Wi-Fi Direct network, after which the check can be resumed. NOTE: The minimum wait time is 60 seconds.
<code>protect-wifi-direct-p2p-groups</code>	Indicates the containment of peers associated with WIFI-Direct GO and devices in a WIFI Direct group, which are connected to a WLAN Infrastructure.

Examples

The following example shows how to execute the `configure terminal` command:

```
(host) # configure terminal
(host) (config) #
```

To return to enable mode, enter `Ctrl-Z` or `exit`.

The following example enables the **Detect WIFI-Direct P2P Groups** parameter:

```
(host) # configure terminal ids unauthorized-device-profile test
```

```
(host) (IDS Unauthorized Device Profile "test")# detect-wifi-direct-p2p-groups
```

The following example configures the wait time for detecting a Wi-Fi Direct network to 120 seconds:

```
(host) # configure terminal ids unauthorized-device-profile test
(host) (IDS Unauthorized Device Profile "test")# wifi-direct-network-quiet-time 120
```

The following example enables the **Protect From WIFI-Direct P2P Groups** parameter:

```
(host) # configure terminal ids unauthorized-device-profile test
(host) (IDS Unauthorized Device Profile "test")# protect-wifi-direct-p2p-groups
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The <code>ids unauthorized-device-profile</code> parameter is introduced.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

controller ble-init-action

```
controller ble-init-action apb-power-reset | clear-all-beacons | clear-all-log-  
mac-filters | clear-log-mac-filter | log-level | log-level-str |log-mac-filter |  
msg-select |  
ota-fw-upgrade | remove-beacon-mac | send-apb-update | send-update | start-log  
| stop-log | zigbee permit-joining restart <all> | <mac>
```

Description

This command will initiate BLE action for controller.

Parameter	Description
apb-power-reset	This parameter will power-on reset for the on-board BLE radio.
clear-all-beacons	This parameter will delete all beacon data.
clear-all-log-mac-filters	This parameter will clear all the BLE daemon log MAC filters.
clear-log-mac-filter	This parameter will clear the BLE daemon log MAC filter.
log-level	BLE daemon log level specified as a number.
log-level-str	BLE daemon log levels specified as comma-separated values (without quotes). Possible values: 'info','warning','error','ageout','bmreq','fw-upgrade',' fw-upgradeerr','cfgupdate','cfgupdateerr','beacon','bcntl v','bcnerr','apb','tags','zf','amon','iot_gw','at-https- json','at-websocket-protobuf'.
log-mac-filter	BLE daemon log MAC filter.
msg-select	Sets bits to enable specific messages from APB to controller BLE Daemon - refer to BLE config CLI command.
ota-fw-upgrade	Over the Air firmware upgrade for onboard BLE.
remove-beacon-mac	Deletes beacon with matching MAC address.
send-apb-update	Sends APB info update to BLE Relay on controller.
send-update	Sends IoT payload message to BMC immediately.
start-log	Enables BLE Daemon logging.
stop-log	Disables BLE Daemon logging.
zigbee permit-joining restart	Re-starts zigbee initial permit joining duration.

Parameter	Description
all	Re-starts all devices.
mac <mac-address>	Re-starts specific devices.

Example

```
(host) [mynode] #controller ble-init-action stop-log
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

controller-ip

```
controller-ip {loopback|vlan <id>}
```

Description

This command sets the IP address of the managed device to the loopback interface address or a specific VLAN interface address.

This command allows you to set the managed device IP to the loopback interface address or a specific VLAN interface address. If the managed device IP command is not configured, the managed device IP defaults to the loopback interface address. If the loopback interface address is not configured, the first configured VLAN interface address is selected. Generally, VLAN 1 is the factory default setting and thus becomes the managed device IP address.

Parameter	Description
loopback	Sets the IP address to the loopback interface. Disabled
vlan <id>	Sets the IP address to a VLAN interface.

Example

The following command sets the IP address to VLAN interface 6.

```
(host) [md] #controller-ip vlan 6
```

Related Commands

Command	Description
show controller-ip	Displays the controller's IP address and VLAN interface ID.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

controller-ipv6

```
controller-ipv6 [loopback|{vlan <VLAN ID>}]  
no ...
```

Description

This command sets the default IPv6 address of the Mobility Conductor to the IPv6 loopback interface address or a specific VLAN interface address.

This command allows you to set the default IPv6 address of the Mobility Conductor to the IPv6 loopback interface address or a specific IPv6 VLAN interface address. If the Mobility Conductor IPv6 command is not configured then the Mobility Conductor IP defaults to the loopback interface address. If the loopback interface address is not configured then the first configured VLAN interface address is selected. Generally, VLAN 1 is the factory default setting and thus becomes the Mobility Conductor IP address.

Parameter	Description
loopback	Sets the managed device IP to the loopback interface. Disabled
vlan	Set the managed device IP to a VLAN interface.
vlan <id>	Specifies the VLAN interface ID.
address <X:X:X:X::X>	Specifies the IPv6 address.

Example

The following command sets the Mobility Conductor IP address to VLAN interface 6:

```
(host) [mynode] (config) #controller-ipv6 vlan 6
```

The following example displays the use of extended scope of address range:

```
(host) [mynode] (config) #controller-ipv6 vlan 294 address 2942::5
```

Related Commands

Command	Description
show controller-ipv6	Displays the Mobility Conductor's IPv6 address and VLAN interface ID.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

copy

copy

```
config sftp <addr> <file> <username>
flash: <srcfilename> {flash: <destfilename>|ftp: <ftphost> <user> [<remote-dir>
[<destfilename>]|scp: <scphost> <username> <destfilename>|tftp: <tftphost>
<destfilename>|usb: partition {0|1} <destfilename>}
ftp: <ftphost> <user> <filename> system: partition {0|1}
running-config {flash: <filename>|ftp: <ftphost> <user> <filename> [<remote-
dir>]|tftp: <tftphost> <filename>}
scp: <scphost> <username> <filename> {flash: <destfilename>|system: partition
{0|1}}
system: partition {<srcpartition> 0|1} [<destpartition> 0|1
sftp <addr> <file> <username> system config
tftp: <tftphost> <filename> {flash: <destfilename>|system: partition {0|1}}
usb: partition <part> <usbfilename> {flash: <flashfilename>|system: partition
{0|1}}
```

copy-provisioning-params

Description

This command copies files to and from the managed device.

Use this command to save back-up copies of the configuration file to an FTP or TFTP server, or to load a saved file from an FTP or TFTP server.

Three partitions reside on the file system flash. Totalling 256MB, the three partitions provide space to hold the system image files (in partitions 1 and 2 which are 45MB each) and user files (in partition 3, which is 165MB). System software runs on the system partitions; the database, DHCP, startup configuration, and logs are positioned on the user partition.

To restore a database, copy the database from the network server and import the database.

To restore a configuration file, copy the file from network server to the managed device's flash system then copy the file from the flash system to the system configuration. This ensures that you do not accidentally overwrite your system startup configuration file.

Unlike the managed device's flash, the USB device has more than two partitions; not just 0 and 1. When copying a file from a USB device, you must know which partition the target file is on. Use the `show storage` command to identify the location of the file to identify the correct USB partition.

Parameter	Description
flash: <srcfilename>	Copies the contents of the managed device's flash file system, the system image, to a specified destination.
flash:	Copies the file to the flash file system.
<destfilename>	New name of the copied file.

Parameter	Description
ftp:	Copies the file to the FTP file system.
<ftphost>	IPv4 or IPv6 address of the FTP server.
<user>	Name of the FTP user.
<remote-dir>	Name of the remote directory.
<destfilename>	New name of the copied file.
scp:	Copies the file to the SCP file system.
<scphost>	IPv4 or IPv6 address of the remote SCP host.
<username>	Username for secure login.
<destfilename>	New name of the copied file.
tftp:	Copies the file to a TFTP server.
<tftphost>	IP address of the TFTP server.
<destfilename>	New name of the copied file.
usb:	Copies the file to an attached USB storage device.
partition	Specifies the partition on the USB device (0,1).
<destfilename>	New name of the copied file.
ftp:	Copies a file from the FTP server.
<ftphost>	IPv4 or IPv6 address or hostname of the FTP server.
<user>	User account name required to access the FTP server.
<filename>	Full name of the file to be copied.
partition	Specifies the system partition to save the file (0,1).
running-config	Copies the active or running configuration to a specified destination.
flash:	Copies the configuration to the flash file system.
<filename>	New name of the copied configuration file.
ftp:	Copies the configuration to an FTP server.
<ftphost>	IP address of the FTP server.

Parameter	Description
<user>	User account name required to access the FTP server.
<filename>	New name of the copied configuration file.
<remote-dir>	Specifies a remote directory, if needed.
startup-config	Copies the active, running configuration to the start-up configuration.
tftp:	Using TFTP, copy the configuration to a TFTP server.
<tftphost>	Specifies the IP address or hostname of the TFTP server.
<filename>	New name of the copied configuration file.
scp:	Copies an ArubaOS image file or file from the flash file system using the Secure Copy protocol. The SCP server or remote host must support SSH version 2 protocol.
<scphost>	IPv4 or IPv6 address of the SCP server or remote host.
<username>	User account name required to access the SCP server or remote host.
<filename>	Absolute path of the filename to be copied.
flash:	Copies the file to the flash file system.
<destfilename>	New name of the copied file.
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).
system:	Copies the specified system partition.
<srcpartition>	Disk partition from which to copy the system data (0,1).
<destpartition>	Disk partition to copy the system data to (0,1).
tftp:	Copies a file from the specified TFTP server to either the controller or another destination. This command is typically used when performing a system restoration, or to pull a specified file name into the wms database.
<tftphost>	IPv4 or IPv6 address of the TFTP server.
<filename>	Full name of the file to be copied.
flash:	Copies the file to the flash file system.

Parameter	Description
<destfilename>	New name of the copied file.
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).
usb:	Copies a file from an attached USB device to the flash file system.
partition <part>	Specifies the partition on the USB device (0,1).
<usbfilename>	Full name of the USB file to be copied.
flash:	Copies the file to the flash file system.
<flashfilename>	New name of the copied file.
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).

Example

The following commands copy the configuration file named "engineering" from the TFTP server to the managed device's flash file system, and then uses that file as the startup configuration. This example assumes the startup configuration file is named default.cfg:

```
(host) [mynode] (config) #copy tftp: 192.0.2.0 engineering flash:
default.bak
copy flash: default.bak flash: default.cfg
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

copy-provisioning-params

```
copy-provisioning-params  
  ap-name <ap-name>  
  ip-addr <ip-addr>
```

Description

This command copies a provisioning-ap-list entry to provisioning-params.

Parameter	Description
ap-name <ap-name>	Specify the AP name for which data provisioning is to be used.
ip-addr <ip-addr>	Specify the IP address for which data provisioning is to be used.

Example

```
(host) [mynode] #copy-provisioning-params ap-name default
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Enable mode on Mobility Conductor.

cp-bandwidth-contract

```
cp-bandwidth-contract <string> pps <1...256000>
```

Description

This command configures a bandwidth contract traffic rate, which can then be associated with a whitelist/allowlist session ACL.

Parameter	Description
<string>	Name of the bandwidth contract.
<1...256000>	Bandwidth rate in packets per second (pps). NOTE: It is recommended that you do not exceed 96000 packets per second or you may encounter buffer allocation issues. 1-256000

Example

The following example configures a bandwidth contract named “cp-rate” with a rate of 100 pps.

```
(host) [mynode] (config) #cp-bandwidth-contract cp-rate pps 100
```

Related Commands

Command	Description
show cp-bwcontracts	Displays a list of control processor bandwidth contracts for whitelist/allowlist ACLs.
firewall cp	This command creates a new whitelist/allowlist ACL and can associate a bandwidth contract with that ACL.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Conductor.

crypto-local isakmp

```
crypto-local isakmp
  allow-via-subnet-routes
  ca-certificate
  certificate-group
  disable-aggressive-mode
  disable-ipcomp
  dpd
  key [peer <peer-ip> | fqdn <ike-id-fqdn>]
  key-hex
  max-allowed-ikev1-exchanges
  max-allowed-negotiations
  permit-invalid-cert
  ppk-add
  ppk-delete
  ppk
  route ipsec
  sa-cleanup
  server-certificate
  use-TPMcert
  xauth
```

Descriptions

This command configures Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Parameter	Description
allow-via-subnet-routes	Configures VIA clients to push subnet routes to Mobility Conductor.
ca-certificate	Assigns the Certificate Authority (CA) certificate used to authenticate VPN clients.
certificate-group	Configures an IKE certificate group for VPN Clients.
disable-aggressive-mode	Disables the IKEv1 aggressive mode.
disable-ipcomp	Disables IP compression on Mobility Conductor.

Parameter	Description
dpd	Configures IKE DPD.
key	Configures the IKE preshared key for site-to-site VPN.
key-hex	Configures the IKE PRE-SHARED key for hex-based characters [0-9,a-f,A-F].
max-allowed-negotiations	Configures the maximum allowed in negotiations value. Exchanges will be throttled after this max limits
max-allowed-ikev1-exchanges	Configures the maximum allowed in-negotiation ikev1 exchanges. Exchanges will be throttled after this max limits.
permit-invalid-cert	Allows invalid or expired certificates to be used for site-to-site VPN.
ppk-add	Configure Postquantum Preshared Key (PPK).
ppk-delete	Delete Postquantum Preshared Key (PPK).
ppk	Configures the IKE Postquantum Preshared Key (PPK).
route ipsec	Configures the subnet route using an IPsec map.
sa-cleanup	Enables the cleanup of IKE SAs.
server-certificate	Assigns the server certificate used to authenticate the Mobility Conductor or managed device for VPN clients using IKEV1 or IKEV2.
use-TPMcert	Use TPM certificate.
xauth	Enables IKE XAuth for VPN clients.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>ppk</code> parameter was introduced.
ArubaOS 8.8.0.0	The <code>maximum-allowed-negotiations</code> parameter was introduced.
ArubaOS 8.0.1.0	The <code>allow-via-subnet-routes</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

crypto-local isakmp allow-via-subnet-routes

crypto-local isakmp allow-via-subnet-routes

Description

This command allows VIA clients to push subnet routes to Mobility Conductor.

Example

This command enables VIA clients to push subnets to Mobility Conductor:

```
(host) [mynode] (config) #crypto-local isakmp allow-via-subnet-routes
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if Mobility Conductor can accept subnet routes from VIA clients.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local ipsec-map

```
crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
  client-mode [<nat>|<network>]
  disable
  dst-net <ipsec-map-dst-net> <mask> | any
  dst-net-ipv6 <ipsec-map-dst-net-ipv6> <ipsec-map-dst-prefix-len>
  enrolled-cert-auth
  factory-cert-auth
  force-natt {enable|disable}
  force-tunnel-mode
  ip access-group {ip <access-group> | session-acl <session acl name>}
  ip-compression {enable|disable}
  ipsec-mtu <mtu>
  load-balance
  local-fqdn <local_id_fqdn>
  monitor <ip> <frequency> <burst count> <retry num>
  no ...
  peer-cert-dn <peer-dn>
  peer-fqdn {any-fqdn|peer-fqdn <peer-id-fqdn>}
  peer-ip <ipaddr>
  peer-ipv6 <ipsec-map-peer-ipv6>
  pre-connect {disable|enable}
  set ca-certificate <cacert-name>
  set ike1-policy <policy-v1-number>
  set ikev2-policy <policy-v2-number>
  set pfs {group1|group2|group14|group19|group20}
  set security-association lifetime kilobytes <kilobytes>
  set security-association lifetime seconds <seconds>
  set server-certificate <cert-name>
  set transform-set <name1> [<name2>] [<name3>] [<name4>]
  src-net <ipsec-map-src-net> vlan <mask> | any
  src-net-ipv6 <ipsec-map-src-net-ipv6> <ipsec-map-src-prefix-len>
  trusted {enable|disable}
  uplink failover {enable|disable}
  version {v1|v2}
  vlan <ipsec-map-vlan-id>
```

Description

This command configures IPsec mapping for site-to-site VPNs.

You can use Mobility Conductor instead of VPN concentrators to connect sites at different physical locations.

You can configure separate CA and server certificates for each site-to-site VPN. You can also configure the same CA and server certificates for site-to-site VPN and client VPN. Use the `show crypto-local ipsec-map` command to display the certificates associated with all configured site-to-site VPN maps; use the **tag <map>** option to display certificates associated with a specific site-to-site VPN map.

Mobility Conductor supports site-to-site VPNs with two statically addressed managed device, or with one static and one dynamically addressed managed device. By default, site-to-site VPN uses

IKE Main-mode with Pre-Shared-Keys to authenticate the IKE SA. This method uses the IP address of the peer, and therefore will not work for dynamically addressed peers.

To support site-site VPN with dynamically addressed devices, you must enable IKE Aggressive-Mode with Authentication based on a Pre-Shared-Key. A managed device with a dynamic IP address must be configured to be the initiator of IKE Aggressive-mode for Site-Site VPN, while the managed device with a static IP address must be configured as the responder of IKE Aggressive-mode.

IKEv2 site-to-site VPNs between Mobility Conductor and 7000 Series Mobility Conductor support traffic compression between those devices. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Skype4b or Voice traffic) is not compromised by increased latency or decreased throughput.

Parameter	Description
<code><map></code>	Name of the IPsec map.
<code><priority></code>	Priority of the entry. 1-9998
<code>client-mode [<nat> <network>]</code>	Enables client-mode where: nat enables nat mode with any and any. network enables network mode
<code>dst-net</code>	IP address and netmask for the destination network.
<code>disable</code>	Disables an existing IPsec map. New maps are enabled by default.
<code>dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask> any</code>	IP address and netmask for the destination network.
<code>dst-net-ipv6 <ipsec-map-dst-net-ipv6> <ipsec-map-dst-prefix-len></code>	IPv6 address and netmask for the destination network.
<code>enrolled-cert-auth</code>	Enables the enrolled certificate authentication for site-to-site tunnel.
<code>factory-cert-auth</code>	Enables factory certificate authentication for site-to-site VPNs. Disabled
<code>force-natt</code>	Include this parameter to always enforce UDP 4500 for IKE and IPsec. This option is disabled by default. Disabled
<code>force-tunnel-mode</code>	Configures the force-tunnel-mode flag.

Parameter	Description
<code>ip access-group</code>	Configures the IP access group name.
<code>ip <access-group></code>	Attaches a route ACL to the IPsec map for a site-to-site VPN. When you associate a routing ACL to inbound traffic on a Mobility Conductor terminating a site-to-site VPN, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group. For more information on creating a routing ACL, see ip access-list route .
<code>session-acl <session acl name></code>	Configures session ACL on IPsec map.
<code>ip-compression</code>	Enable compression for traffic in an IKEv2 site-to-site tunnel between a master/conductor and local 7000 Series Mobility Conductor. Compression is disabled by default. Disabled
<code>ipsec-mtu <mtu></code>	Configures the IPsec MTU of the security association (SA). NOTE: Starting from ArubaOS 8.11.0.0, the supported range has changed from 1024-1500 to 1024-9216 MTU size for an IPsec site-to site tunnel between two managed devices when Jumbo frames are enabled.
<code>load-balance</code>	Enable VPN load balancing for any tunnel. Disabled
<code>local-fqdn <local_id_fqdn></code>	If the managed device has a dynamic IP address, you must specify the FQDN of the managed device to configure it as a initiator of IKE aggressive-mode.
<code>monitor <monitor-ip> interval <interval_secs></code>	Configure link monitor where <monitor-ip> is IP address of monitor server. interval <interval_secs> is optional interval in seconds.
<code>no</code>	Negates a configured parameter.

Parameter	Description
<pre>peer-cert-dn <peer-dn></pre>	<p>If you are using IKEv2 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering its certificate subject name in the Peer Certificate Subject Name field.</p>
<pre>peer-fqdn</pre>	<p>For site-to-site VPNs with dynamically addressed peers, specify a FQDN for the managed device:</p> <ul style="list-style-type: none"> ▪ any-fqdn: Any remote FQDN ID ▪ fqdn-id: Unique remote FQDN ID <pre>any-fqdn</pre>
<pre>peer-ip <ipaddr></pre>	<p>If you are using IKEv1 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering the IP address of the peer gateway.</p> <p>NOTE: If you are configuring an IPsec map for a static-ip managed device with a dynamically addressed remote peer, you must leave the peer gateway set to its default value of 0.0.0.0.</p>
<pre>peer-ipv6 <ipsec-map-peer-ipv6></pre>	<p>If you are using IKEv1 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering the IPv6 address of the peer gateway.</p> <p>NOTE: If you are configuring an IPsec map for a static-ip managed device with a dynamically addressed remote peer, you must leave the peer gateway set to its default value.</p>
<pre>pre-connect</pre>	<p>Enables or disables pre-connection.</p> <pre>disabled</pre>
<pre>set ca-certificate <cacert-name></pre>	<p>User-defined name of a trusted CA certificate installed on the Mobility Conductor. Use the show crypto-local pki TrustedCA command to display the CA certificates that have been imported into the Mobility Conductor. The CA certificate name must be between 1-64 characters in length.</p> <pre>1-64 characters</pre>

Parameter	Description
<pre>set ikev1-policy <policy-v1-number></pre>	Select an IKEv1 policy for the ipsec-map. Predefined policies are described in the table below.
<pre>set ikev2-policy <policy-v2-number></pre>	Select IKEv2 policy for the ipsec-map. Predefined policies are described in the table below.
<pre>set pfs</pre>	<p>If you enable Perfect Forward Secrecy (PFS) mode, new session keys are not derived from previously used session keys. Therefore, if a key is compromised, that compromised key will not affect any previous session keys. To enable this feature, specify one of the following Perfect Forward Secrecy modes:</p> <ul style="list-style-type: none"> ▪ group1: 768-bit Diffie Hellman prime modulus group. ▪ group2: 1024-bit Diffie Hellman prime modulus group. ▪ group14: 2048-bit Diffie Hellman prime modulus group. ▪ group19: 256-bit random Diffie Hellman ECP modulus group. (For IKEv2 only) ▪ group20: 384-bit random Diffie Hellman ECP modulus group. (For IKEv2 only) <p>disabled</p>
<pre>set security-association lifetime kilobytes <kilobytes></pre>	Configures the lifetime for the security association (SA) in kilobytes. 1000 - 1000000000 kilobytes
<pre>set security-association lifetime seconds <seconds></pre>	Configures the lifetime for the security association (SA) in seconds. 300-86400 seconds 7200 seconds
<pre>set server-certificate <cert-name></pre>	User-defined name of a server certificate installed for the site-to-site IPsec map. Use the <code>show crypto-local pki ServerCert</code> command to display the server certificates that have been imported into the Mobility Conductor. The server certificate name must be between 1-64 characters in length.

Parameter	Description
	1-64 characters
<pre>set transform-set <transform-set-name1> [<transform-set-name2>] [<transform-set-name3>] [<transform-set-name4>]</pre>	<p>Name of the transform set for this IPsec map. One transform set name is required, but you can specify up to four transform sets. Configure transform sets with the <code>crypto ipsec transform-set</code> command.</p> <p>transform</p>
<pre>src-net <ipsec-map-src-net> <ipsec-map-src-mask> any</pre>	IP address and netmask for the source network.
<pre>src-net-ipv6 <ipsec-map-src-net-ipv6> <ipsec-map-src-prefix-len></pre>	IPv6 address and netmask for the source network.
<pre>trusted</pre>	<p>Enables a trusted tunnel.</p> <p>NOTE: The <i>trusted <disable></i> sub-parameter is not supported on the managed device. You must always use the <i>trusted <enable></i> sub-parameter so that the traffic can pass through.</p> <p>disabled</p>
<pre>uplink failover</pre>	<p>Enables or disables uplink failover for site-to-site tunnels.</p> <p>disabled</p>
<pre>version</pre>	<p>Select the IKE version for the IPsec map.</p> <ul style="list-style-type: none"> ▪ v1: IKEv1 ▪ v2: IKEv2 <p>v1</p>
<pre>vlan <ipsec-map-vlan-id></pre>	<p>VLAN ID. Enter 0 for the loopback, and 4095 for cellular.</p> <p>1-4094</p>

Understanding Default IKE policies

ArubaOS includes the following default IKE policies. These policies are predefined and cannot be edited.

Table 7: Default IKE Policy Settings

Policy Name	Policy Number	IKE Version	Encryption Algorithm	Hash Algorithm	Authentication Method	PRF Method	Diffie-Hellman Group
Default protection suite	10001	IKEv1	3DES-168	SHA 160	Pre-Shared Key	N/A	2 (1024 bit)
Default Remote AP Certificate protection suite	10002	IKEv1	AES -256	SHA 160	RSA Signature	N/A	2 (1024 bit)
Default Remote AP PSK protection suite	10003		AES -256	SHA 160	Pre-Shared Key	N/A	2 (1024 bit)
Default Remote AP IKEv2 RSA protection suite	1004	IKEv2	AES -256	SSHA160	RSA Signature	hmac-sha1	2 (1024 bit)
Default Cluster PSK protection suite	10005	IKEv1	AES -256	SHA160	Pre-Shared Key	Pre-Shared Key	2 (1024 bit)
Default IKEv2 RSA protection suite	1006	IKEv2	AES - 128	SHA 96	RSA Signature	hmac-sha1	2 (1024 bit)
Default IKEv2 PSK protection suite	10007	IKEv2	AES - 128	SHA 96	Pre-shared key	hmac-sha1	2 (1024 bit)
Default Suite-B 128bit ECDSA protection suite	10008	IKEv2	AES - 128	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)

Policy Name	Policy Number	IKE Version	Encryption Algorithm	Hash Algorithm	Authentication Method	PRF Method	Diffie-Hellman Group
Default Suite-B 256 bit ECDSA protection suite	10009	IKEv2	AES -256	SHA 384-192	ECDSA-384 Signature	hmac-sha2-384	Random ECP Group (384 bit)
Default Suite-B 128bit IKEv1 ECDSA protection suite	10010	IKEv1	AES-GCM-128	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)
Default Suite-B 256-bit IKEv1 ECDSA protection suite	10011	IKEv1	AES-GCM-256	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)



When using a default IKE (V1 or V2) policy for an IPsec map, the priority number should be the same as the policy number.

Examples

The following commands configures site-to-site VPN between two managed devices:

```
(host) [mynode] (config) #crypto-local ipsec-map sf-chi-vpn 100
src-net 101.1.1.0 255.255.255.0
dst-net 100.1.1.0 255.255.255.0
peer-ip 172.16.0.254
vlan 1
trusted

(host) [mynode] (config) #crypto-local ipsec-map chi-sf-vpn 100
src-net 100.1.1.0 255.255.255.0
dst-net 101.1.1.0 255.255.255.0
peer-ip 172.16.100.254
vlan 1
trusted
```

For a dynamically addressed managed device that initiates IKE Aggressive-mode for Site-Site VPN:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-
map-number>
src-net <ipsec-map-src-net> <ipsec-map-src-mask>
dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask>
peer-ip <ipaddr>
local-fqdn <local_id_fqdn>
vlan <ipsec-map-vlan-id>
pre-connect {enable|disable}
trusted enable
For the Pre-shared-key:
crypto-local isakmp key <key> address <ipaddr> netmask <mask>
```

For a static IP managed device that responds to IKE Aggressive-mode for Site-Site VPN:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-
map-number>
src-net <ipsec-map-src-net> <ipsec-map-src-mask>
dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask>
peer-ip 0.0.0.0
peer-fqdn fqdn-id <peer_id_fqdn>
vlan <ipsec-map-vlan-id>
trusted enable
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> fqdn <fqdn-id>
```

For a static IP managed device that responds to IKE Aggressive-mode for Site-Site VPN with One PSK for All FQDNs:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-
map-number>
src-net <ipaddr> <mask>
peer-ip 0.0.0.0
peer-fqdn any-fqdn
vlan <id>
trusted enable
```

For the Pre-shared-key for All FQDNs:

```
crypto-local isakmp key <key> fqdn-any
```

The following example displays the use of extended scope of address range:


```
(host) [mynode] (config) #crypto-local ipsec-map sparta2vesuvius 100
version v2
set ikev2-policy 10009
peer-ipv6 2004::1
peer-cert-dn "/C=US/ST=HI/L=Camp
Smith/O=PACOM/OU=mil/CN=vesuvius.red1.vpn/emailAddress=admin@pacom.mil"
vlan 202
src-net-ipv6 2012:: 64
dst-net-ipv6 2014:: 64
set transform-set "default-gcm256"
set pfs group20
trusted
set ca-certificate red.ca
set server-certificate sparta.red.vpn
!
```

Related Commands

Command	Description
show crypto-local ipsec-map	Displays current IPsec map configurations for site-to-site VPNs.
crypto_local isakmp disable-ipcomp	Globally disables IP compression on all site-to-site VPNs between Mobility Conductor and managed devices by disabling compression from the master/conductor.

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>session-acl <session acl anme></code> sub-parameter was added in the <code>ip access-group</code> parameter.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> enrolled-cert-auth force-tunnel-mode The following parameter was updated: <ul style="list-style-type: none"> <code>ip access-group</code> in <code><access-group></code>
ArubaOS 8.1.0.0	The <code>any</code> sub-parameter was added in <code>dst-net</code> , and <code>src-net</code> parameters. The following parameters were added: <ul style="list-style-type: none"> client-mode load-balance

Release	Modification
	<ul style="list-style-type: none"> ▪ monitor
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The group19 and group20 PFS options requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Config mode on Mobility Conductor.

crypto-local ipsec sa-cleanup

crypto-local ipsec sa-cleanup

Description

Issue this command to clean IPsec security associations (SAs). You can also use this command to remove old IPsec security associations if remote APs on your network still use an old SA after upgrading to a newer version of ArubaOS.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp disable-aggressive-mode

crypto-local isakmp disable-aggressive-mode

Description

The command disables the IKEv1 aggressive mode.

The Mobility Conductor-managed device communication, by default, uses IPsec aggressive mode when a PSK is used for authentication. You need to convert Mobility Conductor-managed device communication to certificate-based IPsec authentication before disabling aggressive mode.

Disabling aggressive mode will impact other sessions that use aggressive mode, such as Conductor-local IKE session with PSK.

Example

```
(host) [mynode] (config) #crypto-local isakmp disable-aggressive-mode
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if aggressive mode is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp ca-certificate

```
crypto-local isakmp ca-certificate <cacert-name>
```

Description

This command assigns the Certificate Authority (CA) certificate used to authenticate VPN clients. You can assign multiple CA certificates. Use the `show crypto-local isakmp ca-certificate` command to view the CA certificates associated with VPN clients.

Parameter	Description
<cacert-name>	User-defined name of a trusted CA certificate installed on the Mobility Conductor. Use the <code>show crypto-local pki TrustedCA</code> command to display the CA certificates that have been imported into the Mobility Conductor.

Example

This command configures a CA certificate:

```
(host) [mynode] (config) #crypto-local isakmp ca-certificate TrustedCA1
```

Related Commands

Command	Description
show crypto-local isakmp	Displays CA certificates configured for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp certificate-group

```
crypto-local isakmp certificate-group server-certificate <server_cert-name> ca-  
certificate <ca_cert-name>
```

Description

The command configures an IKE certificate group for VPN Clients. This feature allows you to create a certificate group so you can access multiple types of certificates on the same Mobility Conductor.

Parameter	Description
server-certificate <server-cert-name>	The IKE server certificate name for VPN clients. 1-64 characters
ca-certificate <ca-cert-name>	The IKE CA certificate for this server certificate. 1-64 characters

Example

This command configures a certificate group that consists of server certificate named "newtest" with the CA certificate "TrustedCA".

```
(host) [mynode] (config) #crypto-local isakmp certificate-group server-  
certificate newtest ca-certificate TrustedCA
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the configured IKE certificate groups for VPN clients.
show crypto-local isakmp	Displays the configured IKE server certificate for VPN clients.
show crypto-local isakmp	Displays the configured IKE CA certificate for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto_local isakmp disable-ipcomp

crypto-local isakmp disable-ipcomp

Description

This command disables IP compression on Mobility Conductor. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Skype4b or Voice traffic) is not compromised by increased latency or decreased throughput.

Example

```
(host) [mynode] (config) #crypto-local isakmp disable-ipcomp
```

Related Commands

Version	Modification
crypto-local ipsec-map	Locally disables IP compression on an individual site-to-site VPN by disabling compression on a specific IPsec map.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp dpd

```
crypto-local isakmp dpd idle-timeout <idle_sec> retry-timeout <retry_sec> retry-attempts <retry_num>
```

Description

This command configures IKE DPD. DPD is enabled by default for site-to-site VPNs.

Parameter	Description
<code>idle-timeout <idle_sec></code>	Idle timeout, in seconds. 10-3600 seconds 22 seconds
<code>retry-timeout <retry_sec></code>	Retry interval, in seconds. 2-60 seconds 2 seconds
<code>retry-attempts <retry_num></code>	Number of retry attempts. 3-10 3

Example

The following command configures DPD parameters:

```
(host) [mynode] (config) #crypto-local isakmp dpd idle-timeout 60 retry-timeout 3 retry-attempts 5
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the IKE DPD configured on a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp key

```
crypto-local isakmp {key <keystring>|key-hex <keystring>}  
  address <peer-address> netmask <mask>  
  addressv6 <peer-addressv6>  
  fqdn <ike-id-fqdn>  
  fqdn-any
```

Description

This command configures the IKE preshared key for site-to-site VPN. This command configures the IKE preshared key.

Parameter	Description
key <keystring>	IKE preshared key value, between 6-64 characters. To configure a pre-shared key that contains non-alphanumeric characters, surround the key with quotation marks. For example: <code>crypto-local isakmp key "key with spaces" fqdn-any</code> .
key-hex <keystring>	IKE preshared key value, between 6-64 hex-based characters. To configure a pre-shared key that contains non-alphanumeric characters, surround the key with quotation marks.
address <peer-address>	IP address for the preshared key.
netmask <mask>	Netmask for the preshared key.
addressv6 <peer-addressv6>	IPv6 address for the preshared key.
fqdn <ike-id-fqdn>	Configures the PSK for the specified FQDN.
fqdn-any	Configures the PSK for any FQDN.

Example

The following command configures an IKE preshared key for site-to-site VPN:

```
(host) [mynode] (config) #crypto-local isakmp key R8nD0mK3y address  
172.16.100.1 netmask 255.255.255.255
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp ppk-add

```
crypto-local isakmp ppk-add
  ppk-id <ppk_id>
  ppk-value
  ppk-value-hex
  ppk-value-hex-tpi1
  ppk-value-hex-tpi2
  ppk-value-tpi1
  ppk-value-tpi2
  peer-any
  peer-fqdn
  peer-ip
  peer-ipv6
  peer-mac
```

Description

This command configures the IKE Postquantum Preshared Key (PPK). This command is limited to site-to-site VPNs.

Parameter	Description
ppk-id <ppk_id>	Configures PPK ID. Must be between 3-256 characters.
ppk-value	Configures ppk value.
ppk-value-hex	Configures the PPK Value in hex characters [0-9,a-f,A-F].
ppk-value-hex-tpi1	Configures first part of ppk value for two person integrity in hex characters [0-9,a-f,A-F].
ppk-value-hex-tpi2	Configures second part of ppk value for two person integrity in hex characters [0-9,a-f,A-F].

Parameter	Description
ppk-value-tpi1	Configures first part of ppk value for two person integrity.
ppk-value-tpi2	Configures second part of ppk value for two person integrity.
peer-any	Configures PPK for any Peer.
peer-fqdn	Configures PPK for peer-fqdn.
peer-ip	Configures PPK for peer IP.
peer-ipv6	Configures PPK for peer IPv6.
peer-mac	Configures PPK for peer MAC.

Example

The following command configures an IKE Postquantum Preshared Key(PPK) for a site-to-site VPN:

```
(host)[mynode] #crypto-local isakmp ppk-add
ppk-id                Configure ppk id

(host) [mynode] #crypto-local isakmp ppk-add ppk-id demo
ppk-value             Configure ppk value
ppk-value-hex        Configure the PPK Value in hex characters [0-
9,a-f,A-F]
ppk-value-hex-tpi1   Configure first part of ppk value for two
person integrity in hex characters [0-9,a-f,A-F]
ppk-value-hex-tpi2   Configure second part of ppk value for two
person integrity in hex characters [0-9,a-f,A-F]
ppk-value-tpi1       Configure first part of ppk value for two
person integrity
ppk-value-tpi2       Configure second part of ppk value for two
person integrity

(host) [mynode] #crypto-local isakmp ppk-add ppk-id demo ppk-value
<ppk_value>          Configure ppk value. Must be between 3-256
characters.

(host) [mynode] #crypto-local isakmp ppk-add ppk-id demo ppk-value
demoval peer-
peer-any              Configure PPK for any Peer
peer-fqdn             Configure peer-fqdn
peer-ip               Configure PPK for peer IP
peer-ipv6             Configure PPK for peer IPv6
peer-mac              Configure PPK for peer MAC
```

Command History

Version	Modification
ArubaOS 8.10.0.0	Parameter introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	The ppk add command is a global action command that should be configured locally, on an individual managed device to perform a PPK-based exchange.

crypto-local isakmp ppk-delete

```
crypto-local isakmp ppk-delete
  ppk-id <ppk_id>
    peer-any
    peer-fqdn
    peer-ip
    peer-ipv6
    peer-mac
```

Description

This command deletes the IKE Postquantum Preshared Key (PPK). This command is limited to site-to-site VPNs.

Parameter	Description
ppk-id <ppk_id>	Configures PPK ID. Must be between 3-256 characters.
peer-any	Deletes PPK for any peer
peer-fqdn	Deletes peer-fqdn
peer-ip	Deletes PPK for peer IP
peer-ipv6	Deletes PPK for peer IPv6
peer-mac	Deletes PPK for peer MAC

Command History

Version	Modification
ArubaOS 8.10.0.0	Parameter introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	The ppk delete command is a global action command that should be configured locally, on an individual managed device to perform a PPK-based exchange.

crypto-local isakmp xauth

crypto-local isakmp xauth

Description

This command enables IKE XAuth for VPN clients.

The `no crypto-local isakmp xauth` command disables IKE XAuth for VPN clients. This command only applies to VPN clients that use certificates for IKE authentication. If you disable XAuth, then a VPN client that uses certificates will not be authenticated using a username and password. You must disable XAuth for Cisco VPN clients using CAC Smart Cards.

Example

This command disables IKE XAuth for Cisco VPN clients using CAC Smart Cards:

```
(host) [mynode] (config) #no crypto-local isakmp xauth
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if IKE XAuth is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

crypto-local isakmp permit-invalid-cert

crypto-local isakmp permit-invalid-cert

Description

This command allows invalid or expired certificates to be used for site-to-site VPN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local pki rcp

```
crypto-local pki rcp <name> [allow-low-assurance-devices|crl-location  
<filename>|enable-ocsp-responder|ocsp-responder-cert <ocsp-responder-cert>|ocsp-  
signer-cert <ocsp-signer-cert>|ocsp-url <ocsp-url>|revocation-check <method1>  
[<method2>]|server-unreachable {revoke-cert|fail-over|allow-cert}]
```

Description

This command specifies the certificates used to sign OCSF for the revocation checkpoint. A revocation checkpoint is automatically created when a TrustedCA or IntermediateCA certificate is imported into Mobility Conductor.

This command allows you to configure the check methods that are used for the given revocation checkpoint. You can configure Mobility Conductor to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client. Refer to the *Certificate Revocation* chapter in the *ArubaOS 8.x User Guide* for more information on how to configure this feature using both the WebUI and CLI.

Parameter	Description
allow-low-assurance-devices	Enables or disables low assurance devices.
crl-location <file>	Location of the CRL that is used for the rcp. The specified CRL filename must be previously imported onto Mobility Conductor before using this option.
enable-ocsp-responder	Enables the OCSP Responder for this revocation checkpoint. The default is disabled.
ocsp-responder-cert <ocsp-responder-cert>	Specifies the certificate that is used to verify OCSP responses. The certificate must be one of the certificate names displayed when the <code>show crypto-local pki OCSPResponderCert</code> command is executed.
ocsp-signer-cert <ocsp-signer-cert>	Specifies the certificate that is used to sign OCSP responses for this revocation checkpoint. The OCSP signer certificate must be previously imported onto Mobility Conductor through the WebUI. The OCSP signer cert can be the same TrustedCA as the checkpoint, a designated OCSP signer certificate issued by the same CA as the checkpoint, or another local trusted authority. If the <code>ocsp-signer-cert</code> is not specified, OCSP responses are signed using the global OCSP signer certificate. If that is not present, an error message is sent out to clients.

Parameter	Description
	<p>NOTE: The OCSP signer certificate (if configured) takes precedence over the global OCSP signer certificate as this is check point specific.</p>
ocsp-url <ocsp-url>	Configures the OCSP Server URL. The URL must be in the form of http://my.responder.com/path . This parameter can contain only one responder URL at time.
revocation-check <method1> [<method2>]	Configures the revocation check methods used for this rcp. Options include: <ul style="list-style-type: none"> ▪ None (default): No revocation checks are performed ▪ CRL: CRL revocation check method ▪ OCSP: OCSP revocation check method You can configure one fallback method.
server-unreachable {revoke-cert fail-over allow-cert}	Configures one of the following methods to use upon failure to connect to the OCSP server: <ul style="list-style-type: none"> ▪ allow-cert: The certificate is considered 'Good' upon failure to establish connection with the OCSP responder server. ▪ fail-over: The certificate revocation is matched against the CRL upon failure to establish connection with the OCSP responder server. ▪ revoke-cert: The certificate is considered 'Revoked' upon failure to establish connection with the OCSP responder server.

Example

This example configures an OCSP client with the OCSP revocation check method and CRL backup method:

```
(host) [mynode] (config) #crypto-local pki rcp CARoot
ocsp-responder-cert RootCA-Ocsp_responder
ocsp-url http://10.4.46.202/ocsp
crl-location file Security1-WIN-05PRNGEKA0-CA-unrevoked.crl
revocation-check ocsp crl
```

Related Commands

Command	Description
crypto-local pki	Configures local certificates, OCSP signer or responder certificates, and Certificate Revocation Lists (CRL). You can also list revocation checkpoints and enable the responder service.
show crypto-local pki	Displays local certificates, OCSP signer or responder certificates, and CRL data and statistics.

Command History

Version	Modification
ArubaOS 8.2.0.0	The <code>allow-low-assurance-devices</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp route ipsec

```
crypto-local isakmp route ipsec <route-ipsec-map-name> { subnet <subnet-val> | vlan <vlan-value> }
```

Description

This command configures the subnet route using an IPsec map. The following example configures a subnet route for VLAN 1 using an IPsec map:

```
(host) [mynode] (config) #crypto-local isakmp route ipsec default-local-master-ipsecmap192.190.189.1 vlan 1
```

Parameter	Description
<route-ipsec-map-name>	Name of the IPsec map.
subnet <subnet-val>	subnet route to be pushed.
vlan <vlan-value>	VLAN for which the subnet route is pushed. Each VLAN must be separated by a comma and dash.

Related Commands

Command	Description
show crypto-local ipsec-map	Displays the list of configured IPsec maps.
show vlan	Displays the list of configured VLANs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp sa-cleanup

crypto-local isakmp sa-cleanup

Description

This command enables the cleanup of IKE SAs. You can also remove expired ISAKMP SAs from the Mobility Conductor using this command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto-local isakmp server-certificate

crypto-local isakmp server-certificate <cert-name>

Description

This command assigns the server certificate used to authenticate the Mobility Conductor or managed device for VPN clients using IKEv1 or IKEv2. This certificate is only for VPN clients and not for site-to-site VPN clients. You can assign separate server certificates for VPN clients using IKEv1 and clients using IKEv2. Use the `show crypto-local isakmp server-certificate` command to view the server certificate associated with VPN clients.



There is a default server certificate installed on Mobility Conductor. However this certificate does not guarantee security for production networks. Best practices is to replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. You can use the WebUI to generate a Certificate Signing Request (CSR) to submit to a CA and then import the signed certificate received from the CA into Mobility Conductor. For more information, see "Managing Certificates" in the *ArubaOS User Guide*.

Parameter	Description
<cert-name>	User-defined name of a server certificate installed on the Mobility Conductor or managed device.

Example

This command configures a server certificate:

```
(host) [mynode] (config) #crypto-local isakmp server-certificate  
MyServerCert
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the server certificates that have been imported into Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto map global-map

```
crypto map global-map <map-number> ipsec-isakmp {dynamic <dynamic-map-name>|ipsec <ipsec-map-name>}
```

Description

This command configures the default global map. This command identifies the dynamic or IPsec map used as the default global map. If you have not yet defined a dynamic or IPsec map, issue the command [crypto map global-map](#) or [crypto-local ipsec-map](#) to define map parameters.

Parameter	Description
<map-number>	Priority of the map.
ipsec-isakmp	Configures an IPsec map.
dynamic <dynamic-map-name>	Uses a dynamic map.
ipsec <ipsec-map-name>	Uses an IPsec map.

Example

The following command configures the global map with the dynamic map named *dynamic_map_2*.

```
(host) [mynode] (config) #crypto map global-map 2 ipsec-isakmp dynamic
dynamic_map_2
```

The following examples display the use of extended scope of address range:

```
(host) [mynode] (config) #crypto map GLOBAL-IKEV2-MAP 10000 ipsec-isakmp
dynamic default-rap-ipsecmap
(host) [mynode] (config) #crypto map GLOBAL-MAP 10000 ipsec-isakmp dynamic
default-dynamicmap
```

Related Commands

Command	Description
show crypto map	Displays IPsec map configurations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto pki-import

```
crypto pki-import
  {der|pem|pfx|pkcs12|pkcs7}
  CRL
  IntermediateCA
  OCSPResponderCert
  OCSPSignerCert
  PublicCert
  ServerCert
  TrustedCA
  <name> <filename> [<passphrase>]
```

Description

The command imports certificates for the captive portal feature and enables installation of a CSR for the Captive Portal feature.

Parameter	Description
der	Import the following certificates in .der (Distinguished Encoding Rule) format.
pem	Import a certificate in X.509 .pem (Privacy-enhanced Electronic Mail) format.
pfx	Import a certificate in .pfx (Personal inFormation eXchange) format.
pkcs12	Import a certificate in .p12 format.
pkcs7	Import a certificate in .p7c format.
CRL	Import a Certificate Revocation List.
IntermediateCA	Import an intermediate Certificate Authority (CA) certificate.
OCSPResponderCert	Import an Online Certificate Status Protocol (OCSP) Responder certificate.
OCSPSignerCert	Import an OCSP Signer certificate.
PublicCert	Import a public certificate.
ServerCert	Import a server certificate.
TrustedCA	Import a trusted CA certificate.
<name> <filename> <passphrase>	<ul style="list-style-type: none">▪ name- Name of the certificate.▪ filename- Original imported file name of the certificate.

Parameter	Description
	<ul style="list-style-type: none"> ▪ passphrase– Optional passphrase for storing the certificate private key. <p>NOTE: The passphrase is not stored in the system. It is used during the import process only.</p>

Example

The following command installs a server certificate in **.der** format.

```
(host) [md] #crypto pki-import der ServerCert cert_20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor

crypto-local pki

```
crypto-local pki
  allow-low-assurance-devices
  CRL <name> <filename>
  global-ocsp-signer-cert
  IntermediateCA <name> <filename>
  OCSPResponderCert <certname> <filename>
  OCSPSignerCert <certname> <filename>
  PublicCert <name> <filename>
  rcp <name>
  ServerCert <name> <filename>
  service-ocsp-responder {enable|disable}
  TrustedCA <name> <filename>
```

Description

This command configures a local certificate, OCSP signer or responder certificate, and Certificate Revocation List (CRL). You can also list revocation checkpoints and enable the responder service.

This command lets you configure the Mobility Conductor to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client. Refer to the *Certificate Revocation* chapter in the *ArubaOS 8.x User Guide* for more information on how to configure this feature using both the WebUI and CLI.

Parameter	Description
allow-low-assurance-devices	Enables or disables low assurance devices.
CRL	Specifies a Certificate Revocation list. Validation of the CRL is done when it imported through the WebUI (requires the CA to have been already present). CRLs can only be imported through the WebUI.
<name>	Name of the CRL.
<filename>	Original imported filename of the CRL.
global-ocsp-signer-cert	Specifies the global OCSP signer certificate used to sign OCSP responses if there is no checkpoint-specific OCSP signer certificate present. If the ocp-signer-cert is not specified, OCSP responses are signed using the global OCSP signer certificate. If this is not present, an error message is sent out to clients. NOTE: The OCSP signer certificate (if configured) takes precedence over the global OCSP signer certificate as this is checkpoint-specific.

Parameter	Description
IntermediateCA	Configures an intermediate CA certificate.
<name>	Name of the intermediate CA certificate.
<filename>	Original imported filename of the CRL.
OCSPResponderCert	Configures an OCSP responder certificate.
<certname>	Name of responder certificate.
<filename>	Original imported filename of the responder certificate.
OCSPSignerCert	Configures an OCSP signer certificate.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
PublicCert	Public key of a certificate. This allows an application to identify an exact certificate.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
rcp <name>	Specifies the revocation checkpoint. A revocation checkpoint is automatically created when a TrustedCA or IntermediateCA certificate is imported on the Mobility Conductor. See crypto-local pki rcp for more details.
ServerCert	Configures a server certificate. This certificate must contain both a public and private key (the public and private keys must match). You can import a server certificate in either PKCS12 or x509 PEM format; the certificate is stored in x509 PEM DES encrypted format on the Mobility Conductor.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
service-ocsp-responder	Enables or disables the OCSP responder service. The default is disabled . To enable this option, a CRL must be configured for this revocation checkpoint, as this is the source of revocation information in the OCSP responses.
TrustedCA	Configures a trusted CA certificate. This can be either a root CA or intermediate CA. Aruba encourages (but does not require) an intermediate CA's signing CA to be the Mobility Conductor itself.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.

Example

The following example configures the Mobility Conductor as an OCSF responder:

```
(host) [mynode] (config) #crypto-local pki service-ocsp-responder
(host) [mynode] (config) #crypto-local pki rcp CARoot
ocsp-signer-cert RootCA-Ocsp_signer
crl-location file Security1-WIN-05PRGNGEKAO-CA-unrevoked.crl
enable-ocsp-responder
```

Related Commands

Command	Description
crypto-local pki rcp	Specifies the certificates that are used to sign OCSF responses for this revocation check point
show crypto-local pki	Displays local certificates, OCSF signer or responder certificates, and CRL data and statistics.

Command History

Version	Modification
ArubaOS 8.2.0.0	The <code>allow-low-assurance-devices</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto dynamic-map

```
crypto dynamic-map <dynamic-map-name> <dynamic-map-number>
  disable
  no ...
  set pfs {group1|group2|group14|group19|group20}
  set security-association lifetime kilobytes <kilobytes>
  set security-association lifetime seconds <seconds>
  set transform-set <name1> [[<name2>] [<name3>] [<name4>]]
  version {v1|v2}
```

Description

This command configures a new or existing dynamic map. Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can optionally associate that map with the default global map using the command [crypto map global-map](#).

Parameter	Description
<dynamic-map-name>	Name of the map.
<dynamic-map-number>	Priority number of the map. 1-10000 10000
disable	Disables the dynamic map.
no	Negates a configured parameter.
set pfs	Enables Perfect Forward Secrecy (PFS) mode. Use one of the following: <ul style="list-style-type: none">▪ group1: 768-bit Diffie Hellman prime modulus group.▪ group2: 1024-bit Diffie Hellman.▪ group14: 2048-bit Diffie Hellman.▪ group19: 256-bit random Diffie Hellman ECP modulus group.▪ group20: 384-bit random Diffie Hellman ECP modulus group. group1
set security-association lifetime seconds <seconds>	Lifetime for the security association (SA) in seconds. 300-86400 7200
set security-association	Lifetime for the security association (SA) in kilobytes.

Parameter	Description
<code>lifetime kilobytes <kilobytes></code>	1000 - 1000000000
<code>set transform-set <name1> [[<name2>] [<name3>] [<name4>]]</code>	Name of the transform set for this dynamic map. You can specify up to four transform sets. You configure transform sets with the crypto ipsec transform-set command. transform
<code>version {v1 v2}</code>	Version of IKE protocol used to set up a security association (SA) in the IPsec protocol suite: <ul style="list-style-type: none"> ▪ v1:IKEv1 ▪ v2: IKEv2 v1

Example

The following command configures a dynamic map:

```
(host) [mynode] (config) #crypto dynamic-map dmap1 100
set pfs group2
set security-association lifetime seconds 300
```

Related Commands

Command	Description
show crypto dynamic-map	Displays IPsec dynamic map configurations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The group19 and group20 PFS options requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Config mode on Mobility Conductor.

crypto ipsec

```
crypto ipsec
  mtu <max-mtu>
  rekey interval <ipsec-rekey-interval>
  transform-set <transform-set-name>
    esp-3des {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes128 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes128-gcm
    esp-aes192 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes256 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes256-gcm
    esp-des {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-null {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
```

Description

This command configures IPsec parameters. Define the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security, and create or edit transform sets that define a specific encryption and authentication type.

Parameter	Description
mtu <max-mtu>	Configure the IPsec Maximum Transmission Unit (MTU) size. <ul style="list-style-type: none">▪ Range—1024-2500▪ Default —1500 NOTE: Starting from ArubaOS 8.10.0.0, the supported range has changed from 1024-1500 to 1024-2500 MTU size.
rekey interval <ipsec-rekey-interval>	Configure IPsec rekey interval. the value can be between 300 to 7200 seconds. The no crypto ipsec rekey interval parameter restores the rekey time to default value.
transform-set <transform-set-name>	Configure a transform set.
transform-set <transform-set-mtu>	Create or modify a transform set.
esp-3des	Use ESP with 168-bit 3DES encryption.
esp-aes128	Use ESP with 128-bit AES encryption.
esp-aes128-gcm	Use ESP with 128-bit AES-GCM encryption.
esp-aes192	Use ESP with 192-bit AES encryption.

Parameter	Description
<code>esp-aes256</code>	Use ESP with 256-bit AES encryption.
<code>esp-aes256-gcm</code>	Use ESP with 256-bit AES-GCM encryption.
<code>esp-des</code>	Use ESP with 56-bit DES encryption.
<code>esp-null</code>	Use ESP with NULL encryption. Supported with only IKEv1.
The following fields are common to the parameters listed in the command definition:	
<code>esp-md5-hmac</code>	Use ESP with the MD5 (HMAC variant) authentication algorithm.
<code>esp-null-hmac</code>	Use ESP with no authentication. This option is not recommended.
<code>esp-sha-hmac</code>	Use ESP with the SHA (HMAC variant) authentication algorithm.

Example

The following command configures 3DES encryption and MD5 authentication for a transform set named **set2**:

```
(host) [mynode] (config)# crypto ipsec transform-set set2 esp-3des esp-md5-hmac
```

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>rekey</code> parameter was introduced.
ArubaOS 8.1.0.0	The <code>esp-null</code> transform-set parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The <code>esp-aes128-gcm</code> and <code>esp-aes56-gcm</code> transform-set parameters require the Advanced Cryptography (ACR) license. All other parameters are available in the base OS.	Config mode on Mobility Conductor.

crypto isakmp

```
crypto isakmp
  block-aruba-ca {enable|disable}
  clear-map
  eap-passthrough {eap-gtc|eap-mschapv2|eap-peap|eap-tls}
  groupname <name>
  initiate-route
  key {key <keystring>|key-hex <keystring-hex>}
  packet-dump {peer <pktdump-peer-ip> | peer-v6 <pktdump-peer-ipv6>}
  policy
  rekey
  udpencap-behind-natdevice {enable|disable}
```

Description

This command configures Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP). Use this command to configure the IKE pre-shared key, set the EAP authentication method for IKEv2 clients using EAP user authentication, and enable source NAT if the IP addresses of clients need to be translated to access the network.

Parameter	Description
block-aruba-ca	Configures the managed device to accept or reject Aruba-certified clients: <ul style="list-style-type: none">▪ enable: Rejects Aruba-certified client certificates and uses custom certificates instead▪ disable: Accepts Aruba-certified client certificates
clear-map	Clear crypto maps that are created by auto-passcode command but not used now.
eap-passthrough	Select one of the following authentication types for IKEv2 user authentication using EAP. <ul style="list-style-type: none">▪ eap-gtc: EAP-GTC authentication method▪ eap-mschapv2: EAP-MSCHAPv2 authentication method▪ eap-peap: EAP-PEAP authentication method▪ eap-tls: EAP-TLS authentication method <p>NOTE: The eap-passthrough parameter allows IKE module to forward the EAP messages between VPN client and external authentication server during tunnel establishment. It is recommended to have a secure channel between ArubaOS and external authentication server to protect sensitive data.</p>

Parameter	Description
groupname <name>	Configures the IKE Aggressive group name. Aggressive-mode IKE is a 3-packet IKE exchange that does not provide identity-protection, but is faster, because fewer messages are exchanged.
initiate-route	Initiate a route to fpapps.
sa	Security Associations
peer <source-ip>	choose an IKE peer.
key {key <keystring> key-hex <keystring-hex>}	Configures the IKE preshared key, which must be 6-64 characters in length: <ul style="list-style-type: none"> ▪ key: Configures the IKE preshared key using text-based characters. ▪ key-hex: Configures the IKE preshared key using hex-based characters (0-9, a-f, A-F).
packet-dump	Enable the packet dump feature for testing.
peer <pktdump-peer-ip>	Configure peer filter for packet dump.
peer-v6 <pktdump-peer-ipv6>	Configure ipv6 peer filter for packet dump.
policy	Configure an IKE policy. [1 - 10015] - 1 highest priority. (priority > 10000 is reserved for default policies)
rekey	Configure IKE rekey interval. The <code>no crypto isakmp rekey interval</code> parameter restores the rekey time to default value.
udpencap-behind-natdevice	Configures NAT-T if the managed device is behind an NAT device (for Windows VPN Dialer only): <ul style="list-style-type: none"> ▪ enable: Enables NAT-T ▪ disable: Disables NAT-T

Example

The following command configures an ISAKMP peer IP address and subnet mask. After configuring an ISAKMP address and netmask, you will be prompted to enter the IKE preshared key.

```
(host) [mynode] (config) #crypto isakmp address 10.3.14.21 netmask 255.255.255.0
Key:*****Re-Type Key:*****
```


Related Commands

Command	Description
show crypto isakmp	Displays IKE parameters configured for ISAKMP.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>rekey</code> parameter was introduced.
ArubaOS 8.5.0.0	A new sub-parameter, <code>eap-gtc</code> was added to the <code>eap-passthrough</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

crypto isakmp policy

```
crypto isakmp policy <priority>
  authentication {pre-share|rsa-sig|ecdsa-256|ecdsa-384}
  disable
  enable [bypass|secret]
  encryption {3DES|AES128|AES192|AES256|DES}
  group {1|2|14|19|20}
  hash {md5|sha|sha1-96|sha2-256-128|sha2-384-192}
  prf {PRF-HMAC-MD5|PRF-HMAC-SHA1|PRF-HMAC-SHA256|PRF-HMAC-SHA384}
  lifetime <seconds>
  no disable
  version {v1|v2}
```

Description

This command configures Internet Key Exchange (IKE) policy parameters for the Internet Security Association and Key Management Protocol (ISAKMP). To define settings for a ISAKMP policy, issue the command `crypto isakmp policy <priority>` then press **Enter**. The CLI will enter **config-isakmp** mode, which allows you to configure the policy values.

Parameter	Description
<priority>	Specifies a number from 1 to 10,000 to define a priority level for the policy. The higher the number, the higher the priority level.
authentication	Configures the IKE authentication method: <ul style="list-style-type: none">▪ pre-share: Preshared key▪ rsa-sig: RSA signatures▪ ecdsa-256: ECDSA-256-bit signatures▪ ecdsa-384: ECDSA-384-bit signatures
disable	Disables the IKE policy.
enable [bypass secret]	Enables the IKE policy using the bypass or secret. Bypass prompts for the enable mode login and password. Secret prompts for the enable password.
encryption	Configures the IKE encryption algorithm: <ul style="list-style-type: none">▪ 3DES: 168-bit 3DES-CBC encryption algorithm▪ AES128: 128-bit AES-CBC encryption algorithm▪ AES192: 192-bit AES-CBC encryption algorithm▪ AES256: 256-bit AES-CBC encryption algorithm▪ DES: 56-bit DES-CBC encryption algorithm
group	Configures the IKE Diffie Hellman group: <ul style="list-style-type: none">▪ 1: 768-bit Diffie Hellman prime modulus group. This is the

Parameter	Description
	default group setting. <ul style="list-style-type: none"> ▪ 2: 1024-bit Diffie Hellman prime modulus group ▪ 14: 2048-bit Diffie Hellman DDH prime modulus group ▪ 19: 256-bit random Diffie Hellman ECP modulus group ▪ 20: 384-bit random Diffie Hellman ECP modulus group
hash	Configures the IKE hash algorithm: <ul style="list-style-type: none"> ▪ md5: MD5 (HMAC variant) hash algorithm ▪ sha: SHA1-160 (HMAC variant) hash algorithm ▪ sha1-96: SHA1-96 (HMAC variant) hash algorithm ▪ sha2-256-128: SHA2-256-128 (HMAC variant) hash algorithm ▪ sha2-384-192: SHA2-384-192 (HMAC variant) hash algorithm
prf	Sets one of the following pseudo-random function (PRF) values for an IKEv2 policy: <ul style="list-style-type: none"> ▪ PRF-HMAC-MD5 (default): MD5 (HMAC variant) PRF ▪ PRF-HMAC-SHA1: SHA1-160 (HMAC variant) PRF ▪ PRF-HMAC-SHA256: SHA2-256 PRF ▪ PRF-HMAC-SHA384: SHA2-384 PRF
lifetime <seconds>	Specifies the lifetime of the IKE security association (SA), from 300 - 86400 seconds.
no disable	Disables the IKE policy.
version	Specifies the version of IKE protocol for the IKE policy: <ul style="list-style-type: none"> ▪ v1: IKEv1 ▪ v2: IKEv2

Example

The following command configures the RSA signature authentication method for the given IKE policy:

```
(host) [mynode] (config) #crypto isakmp policy 1
(host) [mynode] (config-isakmp) #authentication rsa-sig
Key:*****Re-Type Key:*****
```

Related Commands

Command	Description
show crypto isakmp	Displays IKE policies configured for ISAKMP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	<p>The following settings require the Advanced Cryptogram (ACR) license:</p> <ul style="list-style-type: none"> ▪ hash algorithm: SHA-256-128, SHA-384-192 ▪ Diffie-Hellman (DH) Groups: 19 and 20 ▪ Pseudo-Random Function (PRF): PRF-HMAC-SHA256, PRF-HMAC-SHA384 ▪ Authentication: ecdsa-256 and ecdsa-384 <p>All other parameters are supported in the base OS.</p>	Config mode on Mobility Conductor.

crypto pki

```
crypto pki
  csr {ec|rsa}
    key_len <key_val>
    curve-name <key_val>
    common_name <common_val>
    country <country_val>
    state_or_province <state>
    city <city_val>
    organization <organization_val>
    unit <unit_val>
    email <email_val>
  expirycheck
  export ca-cert pem self-signed {console|<filename>}
```

Description

This command generates a Certificate Signing Request (CSR) for the captive portal feature. Use this command in enable mode to generate a CSR for the Captive Portal feature or to see all managed devices certificates that are expiring.

Displays the CSR output by entering the command `show crypto pki csr`.

Parameter	Description
<code>csr {ec rsa}</code>	Generate a certificate signing request. Execute the <code>show crypto pki csr</code> command to view output again. This parameter has the following sub-parameters: <ul style="list-style-type: none">▪ <code>ec</code>- Generate a certificate signing request with an Elliptic Curve (EC) key.▪ <code>rsa</code>- Generate a certificate signing request with a Rivest, Shamir and Adleman (RSA) key.
<code>key_len <key_val></code>	Generate a certificate signing request with an RSA key with one of the following supported RSA key lengths: <ul style="list-style-type: none">▪ 1024▪ 2048▪ 4096
<code>curve-name <key_val></code>	Generate a certificate signing request with an EC key, with one of the following EC types: <ul style="list-style-type: none">▪ <code>secp256r1</code>▪ <code>secp384r1</code>
<code>common_name <common_val></code>	Specify a common name, e.g., <code>www.yourcompany.com</code> .

Parameter	Description
country <country_val>	Specify a country name, e.g., US or CA.
state_or_province <state>	Specify the name of a state or province.
city <city_val>	Specify the name of a city.
organization <organization_val>	Specify the name of an organization unit, e.g., sales.
unit <unit_val>	Specify a unit value, e.g. EMEA.
email <email_val>	Specify an email address, in the format name@mycompany.com.
expirycheck	Run an expiry check on all certificates on the managed device.
export	Export self signed PKI CA certificate in .pem format.

Example

The following command configures a CSR for a user with the email address *jdoe@example.com*.

```
(host) [md] #crypto pki csr key 1024 common_name www.example.lcom country US state_or_province ca city Sunnyvale organization engineering unit pubs email jdoe@example.com
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

database synchronize

```
database synchronize
  captive-portal-custom
  period <minutes>
```

Description

This command configures the Mobility Conductor to synchronize the database with a standby or backup Mobility Conductor. This command should be executed from the **/mm** node hierarchy. The command takes effect immediately. Use the `database synchronize period` command in config mode to configure the interval for automatic database synchronization.

Parameter	Description
<code>captive-portal custom</code>	Synchronizes custom captive portal files.
<code>period</code>	Configures the interval for automatic database synchronization.
<code><minutes></code>	Interval, in minutes. Range is 1 — 25200 minutes.

Example

The following command causes the database on the active Mobility Conductor to synchronize with the standby in 25 minute intervals.

```
(host) [mynode] (config) #database synchronize period 25
```

Related Commands

Command	Description
database-synchronize	This command synchronizes the Mobility Conductor database with a standby or backup Mobility Conductor.
show database	This command displays database synchronization status.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

datapath

```
datapath {coredump | dns-cache periodic-flush <interval> <threshold> | energy-efficiency}
```

Description

This command configures datapath options.

Parameter	Description
coredump	Generates a coredump, which is a copy of the datapath memory, in the event that the datapath times out. This copy is saved in the system memory.
dns-cache periodic-flush	Configures time period to check if the dns iplist table has reached the configured threshold level.
<interval>	Time interval to check the dns-cache-table threshold. Range: 1 to 24 hours
<threshold>	Threshold limit after which the dns-cache-table will be cleared. Range: 50 to 99 percentage
energy-efficiency	Minimizes idle CPU spinning.

Example

The following command enables datapath coredump:

```
(host) [mynode] (config) #datapath coredump
```

Command History

Release	Description
ArubaOS 8.5.0.7	The dns-cache periodic-flush <interval> <threshold> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

database-synchronize

database-synchronize

Description

This command synchronizes the Mobility Conductor database with a standby or backup Mobility Conductor.

This command should be executed from the enable mode of the Mobility Conductor and takes effect immediately. If a peer is not configured, the Mobility Conductor displays an error message **Cannot start database synchronization: peer is not configured.**

Example

The following command invokes the database on the active Mobility Conductor to synchronize with the standby:

```
(host) [mynode] #database-synchronize
```

Related Commands

Command	Description
database synchronize	This command configures the Mobility Conductor to synchronize the database with a standby or backup Mobility Conductor. This works in config mode.
show database	This command displays database synchronization status.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

dds trace

```
dds trace {receive|transmit} [channel <channel>|peer <A.B.C.D>|peerv6 <X:X:X:X::X>]
```

Description

This command configures trace events.

Parameter	Description
receive	Configures trace receiving events.
transmit	Configures trace transmitting events.
channel	GSM channel for tracing.
<channel>	Name of GSM channel.
peer	DDS peer.
<A.B.C.D>	Peer IP address.
peerv6	DDS IPv6 peer.
<X:X:X:X::X>	Peer IPv6 address.

Example

The following command configures a trace receiving event for the radio GSM channel. Use the `show gsm channel` command to view the list of available GSM channels.

```
(host) [mynode] (config) #dds trace receive channel radio peer 10.20.22.17
```

Command History

Release	Description
ArubaOS 8.2.0.0	The <code>peerv6</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

delete

```
delete
  filename <filename>
  ssh-host-addr <ipaddr>
  ssh-known-hosts
```

Description

This command deletes a file or RSA signature entry from flash. To prevent running out of flash file space, you should delete files that you no longer need. The `copy scp` command creates RSA signatures whenever it connects to a new host. These host signatures are stored in the flash file system.

Parameter	Description
filename	<p>Name of the file to be deleted.</p> <p>Filenames can be specified in the below formats:</p> <ul style="list-style-type: none">▪ To specify filename listed in 'dir' command <code>delete filename <file-name></code>▪ To specify filename listed in 'dir flash' with complete path <code>delete filename <flash_file_path/file-name></code>▪ To delete multiple files with similar filenames, use 'asterisk' in the end <p>For example, <code>delete filename test*</code>: all file names beginning with test will be deleted from /flash/config folder.</p> <p>For example, <code>delete filename <flash_file_path>/test*</code>: all filenames beginning with test will be deleted from <flash_file_path> folder.</p> <p>NOTE: Only files listed in <code>dir</code> and <code>dir flash</code> can be deleted.</p>
ssh-host-addr	Deletes the entry stored in flash for the RSA host signature created when you run the <code>copy scp</code> command.
ssh-known -hosts	Deletes all entries stored in flash for the RSA host signatures created when you run the <code>copy scp</code> command.

Example

The following command deletes a file:

```
(host) [mynode] #delete filename december-config-backup.cfg
```

The following command deletes an RSA signature entry from flash:

```
(host) [mynode] #delete ssh-host-addr 10.100.102.101
```

The following command deletes all RSA signature entries from flash:

```
(host) [mynode] #delete ssh-known-hosts
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

delete-wired-blacklist-user / delete-wired-denylist-user

delete-wired-blacklist-user / delete-wired-denylist-user mac <macaddr>

Description

This command deletes a wired user from blacklist/denylist table.

Parameter	Description
mac <macaddr>	MAC address, in the format xx:xx:xx:xx:xx:xx.

Example

The following command deletes a wired user from blacklist/denylist table:

```
(host) [mynode] #delete-wired-blacklist-user 00:0b:86:f0:05:60
(host) [mynode] #delete-wired-denylist -user 00:0b:86:f0:05:60
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

dir

```
dir
  date
  flash
  name
  search
  size
  usb:
```

Description

This command displays a list of files stored in the flash file system.

Use this command to view the system files associated with the Mobility Conductor. To view the system file associated with the managed device, login to the Mobility Conductor and initiate a telnet or SSH session to the managed device.

Parameter	Description
date	Sort the directory contents by date
flash	list the /flash directory contents
name	Sort the directory contents by name
search	Filter the directory contents by keyword
size	Sort the directory contents by size
usb:	Displays the files in the external USB. NOTE: This parameter can be executed for managed devices that have an USB port.

Output from this command includes the following:

- The first column contains ten place holders that display the file permissions.
 - First place holder: Displays - for a file or **d** for directory.
 - Next three place holders: Display file owner permissions: **r** for read access, **w** for write access permissions, **x** for executable.
 - Following three place holders: Display member permissions: **r** for read access or **x** for executable.
 - Last three place holders: Display non-member permissions: **r** for read access or **x** for executable.
- The second column displays the number of links the file has to other files or directories.

- The third column displays the file owner.
- The fourth column displays group/member information.
- The remaining columns display the file size, date and time the file was either created or last modified, and the file name.

Example

The following command displays the files currently residing on the system flash:

```
(host) [mynode] #dir
```

The following is sample output from this command:

```
-rw-r--r-- 1 root root 9338 Nov 20 10:33 class_ap.csv
-rw-r--r-- 1 root root 1457 Nov 20 10:33 class_sta.csv
-rw-r--r-- 1 root root 16182 Nov 14 09:39 config-backup.cfg
-rw-r--r-- 1 root root 14174 Nov 9 2005 default-backup-11-8-05.cfg
-rw-r--r-- 1 root root 16283 Nov 9 12:25 default.cfg
-rw-r--r-- 1 root root 22927 May 25 12:21 default.cfg.2016-05-25_20-21-38
-rw-r--r-- 2 root root 19869 May 9 12:20 default.cfg.2016-05-09_12-20-22
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

disaster-recovery

```
disaster-recovery
  off
  on
```

Description

This command enables or disables disaster recovery mode on the managed device.

This command is used to recover operations on a managed device that has inherited an incorrect configuration from the Mobility Conductor and can no longer communicate with the Mobility Conductor. When disaster-recovery is enabled, the configuration inherited from the Mobility Conductor can be modified locally on the managed device. When disaster-recovery mode is disabled, the managed device will synchronize its configuration with the Mobility Conductor and any local configuration changes on the managed device will be overwritten.

An example could be a configuration change on the Mobility Conductor that has modified VLAN or port information on the managed device that breaks the IPSEC connection between them. An administrator can enable disaster-recovery mode and correct the configuration on the managed device to restore connectivity to the Mobility Conductor.

Parameter	Description
off	Disables disaster recovery mode.
on	Enables disaster recovery mode.

Example

The following command enables the disaster recovery mode in the managed device:

```
(host-md) #disaster-recovery on
*****
Entering disaster recovery mode
*****
(DR-Mode) [mm] #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed device.

disable-crc-workaround

disable-crc-workaround

Description

Starting from ArubaOS 8.6.0.7, users can issue the `disable-crc-workaround` command when port flaps of the uplink switch are not detected by the Mobility Master. This command dumps all the PHY register data like alarms, warnings, signal strength and hence, will be helpful for debugging.

It is to be noted that when this configuration is enabled, the CRC workaround will be initiated only when the uplink switch shuts down and come up and not when the the device is stable.

Example

```
(host) [mynode] (config) #disable-crc-workaround
```

Command History

Release	Description
ArubaOS 8.7.1.1	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

disable-whitelist-sync / disable-allowlist-sync

disable-whitelist-sync / disable-allowlist-sync

Description

This command disables whitelist/allowlist synchronization with managed devices and it is enabled by default.

Once the entries are synchronized across all controllers, issue the `disable-whitelist-sync / disable-allowlist-sync` command to disable synchronization. Configuring this parameter reduces the number of database queries on Mobility Conductor.



Enabling whitelist/allowlist database synchronization may increase database process CPU utilization on Mobility Conductor if there is a large number of entries and managed devices terminating on the Mobility Conductor.

Example

The following command disables whitelist/allowlist synchronization:

```
(host) [mynode] (config) #disable-whitelist-sync / disable-allowlist-sync
```

Command History

Release	Description
ArubaOS 8.9.0.0	The following terminologies are updated: <ul style="list-style-type: none">▪ All instances of <code>master</code> have been replaced with <code>conductor</code>.▪ All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

dot1x

```
dot1x
  eap-frag-mtu <eapfragmtu>
  high-watermark <1-32000>
  stm-throttling percent <10-80>
```



Use this command only under the supervision of Aruba support.

Description

Use this command under the guidance of Aruba support to configure the maximum and minimum thresholds for the table that contains 802.1X sessions.

Parameter	Description
<code>eap-frag-mtu <eapfragmtu></code>	Enables fragmentation of EAP packets in non-term mode towards EAP server
<code>high-watermark</code>	The maximum entries in the Active table. When the number of entries in the Active table reaches the High Water Mark value, new requests are queued on the Pending table. 1-32000 entries
<code>stm-throttling-percent <10-80></code>	Enables STM throttling when the total entries in the Pending table are greater than (stm-throttling percent) * (high watermark). The default STM throttling percent is 50%. 10-80%

Example

The following command sets the **High Water Mark** value to 200 entries:

```
(host) [mynode] (config) #dot1x high-watermark 200
```

Related Commands

Command	Description
<code>show dot1x watermark</code>	Displays information about the table that contains 802.1X sessions.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

dot1x-transactions-monitor

```
dot1x-transactions-monitor
  start
  stop
```

Description

This command starts or stops the display of the rate statistics using the `show dot1x-transactions-monitor` command. After setting the interval and duration of the rate statistics, enable the start option to start the rate statistics in the `show dot1x-transactions-monitor` command output. To stop the running statistics, manually enter the stop command in the `dot1x-transactions-monitor` command.

Parameter	Description
<start>	Starts the rate statistics in the <code>show dot1x-transactions-monitor</code> command output.
<stop>	Stops the rate statistics in the <code>show dot1x-transactions-monitor</code> command output.

Example

The following command sets the interval and duration of stats for a 802.1X user:

```
(host) [mynode] (config) #dot1x-transactions-monitor 15 55
```

Related Commands

Command	Description
dot1x-transactions-monitor set	Sets the rate statistics interval duration and the total duration of a 802.1X transaction.
show dot1x-transactions-monitor	Displays the rate statistics for a 802.1X user.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

dot1x-transactions-monitor set

```
dot1x-transactions-monitor set <interval> <duration>
```

Description

This command allows the user to provide the rate statistics interval duration and the total duration of a 802.1X transaction.

Parameter	Description
<interval>	Sets the interval for performance test.
<duration>	Sets the duration, in seconds, for performance test. Range: 5-60

Example

The following command sets the interval and duration of stats for a 802.1X user:

```
(host) [mynode] (config) #dot1x-transactions-monitor set 15 55
```

Related Commands

Command	Description
dot1x-transactions-monitor	Starts or stops the display of the rate statistics using the <code>show dot1x-transactions-monitor</code> command.
show dot1x-transactions-monitor	Displays the rate statistics for a 802.1X user.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

downloadable-role-delete

downloadable-role-delete STRING

Description

This command deletes a corrupted role downloaded from ClearPass Policy Manager.

You can delete a downloadable role under the following conditions:

- If no user references the role.
- If the role is in **Complete** or **Incomplete** state.

Parameter	Description
STRING	Downloadable role name.

Example

The following command deletes the *abc_profile-3023-8* user role:

```
(host) [mynode] #downloadable-role-delete abc_profile-3023-8
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

dpi

dpi

```
app <string> ports [tcp <tportlist>][udp <uportlist>]
appcategory <string> <categoryID>
custom-app <appname> <appid> [appcategory|http {hostname-param <hostname> uri-
  param <uri>|referrer-param <referrer>}|https {common-name <commonname>}]
global-bandwidth-contract {app <string>[downstream|upstream] [kbits
  <256..2000000>|mbits <1..2000>}|appcategory <string>[downstream |upstream]
  [kbits|mbits <value>]}
```

Description

This command configures DPI and the global bandwidth contract for an application or application category for the AppRF feature, and allows network administrators to define custom applications for use with DPI features.

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Applications and application categories can be user-defined. Issue the `show dpi custom-app all` command to view all user-defined (custom) applications and the `show dpi application category user-defined all` command to view all user-defined categories.

Parameter	Description
app <string>	Name of the application for which you want to enable DPI. For a complete list of supported applications, issue the command <code>show dpi application all</code> .
tcp <tportlist>	Enables DPI on the selected TCP port(s). You can enter a range of ports (for example, 80-85), or enter multiple individual port numbers separated by a comma (or example, 40,44,48).
udp <uportlist>	Enables DPI on the selected TCP port(s). You can enter a range of ports (for example, 80-85), or enter multiple individual port numbers separated by a comma (or example, 40,44,48).
appcategory	Configures an application category.
<string>	Name of the application category. Allowed characters include: <ul style="list-style-type: none">▪ a-z▪ 0-9▪ "_" and "-"
<categoryid>	Sets a unique category ID.

Parameter	Description
	1-32
custom-app	Creates a new custom application.
<appname>	Name of the custom application. Allowed characters include: <ul style="list-style-type: none"> ▪ a-z ▪ 0-9 ▪ " " ▪ -
<appID>	Sets a unique application ID. 1-64
appcategory	Application category name.
http	Creates a new HTTP-based custom application
hostname-param <hostname> uri-param <uri>	Specifies a hostname and URI to create an application based upon that server name and URI
referrer-param <referrer>	A referrer is the URL of a webpage from which a link was followed. Specify a referrer to create a HTTP referrer-based application.
https	Create a new HTTPS-based custom application
common-name <commonname>	Specify a CN to create an application based on it.
global-bandwidth-contract	Configures the global bandwidth contract for an application or application category. 256 kbps-2 gbps
app <string>	Name of the application. For a complete list of supported applications, issue the command <code>show dpi application all</code> . Applications can also be user-defined. Issue the <code>show dpi custom-app all</code> command to view all user-defined (custom) applications.
appcategory <string>	Name of the application category. For a complete list of supported application categories, issue the command <code>show dpi application category all</code> . Application categories can also be user-defined. Issue the <code>show dpi application category user-defined all</code> command to view all user-defined (custom) categories.
downstream	Bandwidth contract to downstream traffic.

Parameter	Description
upstream	Bandwidth contract to upstream traffic.
kbits <value>	Specifies bandwidth in kbits per second. 256-2000000 kbits
mbits <value>	Specifies bandwidth in mbits per second. 1-2000 mbits

Example

The following command configures a global bandwidth contract for downstream traffic:

```
(host) [md] (config) #dpi global-bandwidth-contract appcategory web
downstream kbits 10000
```

Use the following commands to view global bandwidth contract configuration outputs:

```
(host) [md] #show dpi global-bandwidth-contract all
(host) [md] #show dpi global-bandwidth-contract application name
(host) [md] #show dpi global-bandwidth-contract appcategory name
```

Related Commands

Command	Description
show dpi	Displays the applications and application categories that are configured for Deep-Packet Inspection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

drop-cache

drop-cache

Description

This command frees unused or dirty memory from Mobility Conductor.

This command can be executed when Mobility Conductor has low memory. Execute this command under the supervision of Aruba TAC.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

drt-zwdfs

drt-zwdfs {enable | disable}

Description

This command enables or disables zero wait Dynamic Frequency Selection (DFS) in Downloadable Regulatory Table (DRT).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

dump-collection-profile

```

dump-collection-profile
  clone <source>
  dump-auto-uploading-profile
  dynamic-pcap-interval <dynamic-pcap-interval>
  NO
  server-ip <server-ip>
  server-password <server-password>
  server-path <server-path>
  server-port <server-port>
  server-username <server-username>
  system-dump-enable
  transfer-enable
  transfer-mode {scp | tftp | USB-Transfer}

```

Description

This command configures a dump collection profile.

Parameter	Description
clone <source>	Copy data from specified dump collection profile.
dump-auto-uploading-profile	Configures the dump auto uploading profile.
dynamic-pcap-interval <dynamic-pcap-interval>	Specify the dynamic pcap collection interval in minutes. This value can be from 0 to 30 minutes. To disable the dynamic pcap collection, set this interval value to 0.
NO	Delete command
server-ip <server-ip>	Specify IP address of the server for dump collection.
server-password <server-password>	Specify the server password for dump collection.
server-path <server-path>	Specify the server file path for dump collection.
server-port <server-port>	Server Port for Dump Collection
server-username <server-username>	Server Username for Dump Collection
system-dump-enable	Enable Collection of System Dump in case of AP Crash

Parameter	Description
transfer-enable	Enable transfer of collected file.
transfer-mode {scp tftp USB-Transfer}	Specify one of the following mode to transfer dump files: <ul style="list-style-type: none"> ■ scp: Dump files will be transferred using SCP. ■ TFTP: Dump files will be transferred using TFTP. ■ USB-Transfer: Dump files will be copied to connected USB device in case of a crash.

The following command configures the dump collection profile:

```
(host) [mynode] (config) #dump-collection-profile default
(host) [mynode] (Dump collection profile "default") #
clone                               Copy data from another Dump collection profile
dump-auto-uploading-profile         Dump auto uploading profile
dynamic-pcap-interval              Dynamic pcap collection interval [mins]. Range
0-30. 0:disabled
no                                  Delete Command
server-ip                          Server IP(v4/v6) for Dump Collection
server-password                    Server Password for Dump Collection
server-path                        Server File Path for Dump Collection
server-port                        Server Port for Dump Collection
server-username                    Server Username for Dump Collection
system-dump-enable                 Enable Collection of System Dump in case of AP
Crash
transfer-enable                    Enable Transfer Collected File
transfer-mode                       Configure Dump Transfer Mode
```

The following command configures the dump auto uploading profile.

```
(host) [mynode] (config) #dump-auto-uploading-profile test
(host) [mynode] (Dump Auto Uploading profile "test") #
clone                               Copy data from another Dump Auto Uploading profile
no                                  Delete Command
nss-dump-enable                    Enable Collect nssddr, nssimem Dump Files
radio-dump-enable                  Enable Collect imem, q6mem, QCN9000 Dump Files
```

Command History

Release	Modification
ArubaOS 8.11.1.0	The dump-auto-uploading-profile parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

dynamic-ip

dynamic-ip restart

Description

This command restarts the PPPoE or DHCP process.

This command can be used to renegotiate DHCP or PPPoE parameters. This can cause new addresses to be assigned on a VLAN where the DHCP or PPPoE client is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

eject usb

```
eject usb: slot {all|<slotno>}
```

Description

This command ejects an external USB device from the managed device. Use this command to safely remove an external USB device. This command should be executed from the managed device only.

Parameter	Description
all	Eject all external USB devices.
<slotno>	Enter optional slot number to eject the USB device.

Example

This command ejects all external USB devices from the managed device.

```
(host-md) #eject usb: slot all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

encrypt

encrypt {disable|enable}

Description

This command allows passwords and keys to be displayed in plain text or encrypted. Certain commands, such as `show crypto isakmp key`, display configured key information. Use the `encrypt` command to display the key information in plain text or encrypted.

Parameter	Description
disable	Passwords and keys are displayed in plain text.
enable	Passwords and keys are displayed in encrypted form. enabled

Example

The following command allows passwords and keys to be displayed in plain text:

```
(host) [mynode] #encrypt disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

esi group

```
esi group <group_inst> [ping <attributes>|server <server>]
```

Description

This command configures an ESI group. Use the `show esi groups` command to view ESI group information.

Parameter	Description
<group_inst>	Specifies the ESI group configuration.
no	Delete the command.
ping <ping>	Specifies a set of ping checking attributes. Only one set is allowed.
server <server>	Adds or removes a server from the ESI group.

Example

The following command sets up the ESI group named “fortinet”:

```
(host) [md] (config) #esi group fortinet
ping default
server forti_1
```

Related Commands

Command	Description
show esi groups	Displays ESI group information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

esi parser domain

```
esi parser domain <domain-name>  
  peer <peer-ip>  
  server <ipaddr>
```

Description

This command configures an ESI syslog parser domain. The ESI parser is a generic syslog parser that accepts syslog messages from external third-party appliances, such as anti-virus gateways, content filters, and intrusion detection systems. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers (see [esi server on page 622](#)) are configured into domains to which ESI syslog parser rules (see [esi parser rule on page 616](#)) are applied.

Parameter	Description
<domain-name>	ESI parser domain name.
no	Delete the command.
peer <peer-ip>	Specifies the IP address of an another managed device in this domain, which is notified when the user cannot be found locally. This command is required only when multiple managed devices share a single ESI server.
server <ipaddr>	Specifies the IP address of the ESI server to which the managed device listens.

Example

The following commands configure a virus syslog parser domain named “fortinet” that contains the ESI server “forti_1” with a trusted IP address:

```
(host) [md] (config) #esi parser domain fortinet  
server 10.168.172.3
```

Related Commands

Command	Description
show esi parser	Displays information about the ESI parser domains.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

esi parser rule

```
esi parser rule <rule_name>
  condition <string>
  domain <word>
  enable
  match {ipaddr <string>|mac <string>|user <string>}
  no
  position <1-32>
  set {denylist/blacklist|role <word>}
  test {msg <syslog>|file <filename>}
```

Description

This command creates or changes an ESI syslog parser rule. The user creates an ESI rule by using characters and special operators to specify a pattern that uniquely identifies a syslog message. This “condition” defines the type of message and the ESI domain to which this message pertains. The rule contains three major fields:

- **Condition:** The pattern that uniquely identifies the syslog message type.
- **User:** The username identifier. It can be in the form of a name, MAC address, or IP address.
- **Action:** The action to take when a rule match occurs.

Once a condition match occurs, no further rule-matching will be made. For the matching rule, only one action can be defined.

For more details on the character-matching operators, repetition operators, and expression anchors used to defined the search or match target, refer to the *External Services Interface* chapter in the *ArubaOS 8.x User Guide* .

Use the `show esi parser rules` command to show ESI parser rule information. Use the `show esi parser stats` command to show ESI parser rule statistical information.

Parameter	Description
<rule-name>	Name of the ESI parser rule.
condition <string>	Specifies the REGEX (regular expression) pattern that uniquely identifies the syslog.
domain <word>	(Optional) Specifies the ESI syslog parser domain to which this rule applies. If not specified, the rule matches with all configured ESI servers.
enables	Enables this rule. NOTE: The condition, user match, and set action parameters must be configured before the rule can be enabled.

Parameter	Description
	Disabled
match	Specifies the user identifier to match, where ipaddr , mac , and user take a REGEX pattern that uniquely identifies the user.
ipaddr <string>	Matches using the client IP address.
mac <string>	Matches using the client MAC address.
user <string>	Matches using the client user name.
no	Negates any configured parameter.
position	Specifies the rule's priority position. 1–32; 1 highest
set	Specifies the action to take. NOTE: The role entity should be configured before it is accepted by the ESI rule.
blacklist/denylist	Blocks the user.
role <word>	Changes the user role.
test	Tests the regular expression output configured in the <code>esi parser rules</code> command.
msg <syslog>	Tests the rule against a syslog message.
file <filename>	Tests the rule against a syslog file.

Examples

The following command sets up the Fortigate virus rule named "forti_rule." This rule parses the virus detection syslog scanning for a condition match on the log_id value (log_id=) and a match on the IP address (src=).

```
(host) [md] (config) #esi parser rule forti_rule
condition "log_id=[0-9]{10}[ ]"
match ipaddr "src=(.*)[ ]"
set blacklist/denylist
domain fortinet
enable
```

In this example, the corresponding ESI expression is:

```
< Sep 26 18:30:02 log_
id=0100030101 type=virus subtype=infected src=1.2.3.4 >
```

The following example of the test command tests a rule against a specified single syslog message:

```
(host) [md] (config) #esi parser rule test msg "26 18:30:02 log_
id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:      Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following example of the test command tests a rule against a file named test.log, which contains several syslog messages:

```
(host) [md] (config) #esi parser rule test file test.log

< Sep 26 18:30:02 log_
id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:      Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====

< Oct 18 10:43:40 cli[627]: PAPI_
Send: To: 7f000001:8372 Type:0x4 Timed out. >
=====
Condition:      No matching rule condition found
=====

< Oct 18 10:05:32 mobileip
[499]: <500300> <DEBUG> |mobileip| Station 00:40:96:a6:a1:a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_
DHCP_NO_PROXY, next: PROXY_DHCP_NO_PROXY >
=====
Condition:      No matching rule condition found
=====
```

Related Commands

Command	Description
show esi parser	Displays configuration information for the ESI parser rules.
show esi parser	Displays statistics information for the ESI parser rules.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

esi ping

```
esi ping <ping_inst>
  frequency <frequency_inst>
  no
  retry-count <retry-count_inst>
  timeout <timeout_inst>
```

Description

This command specifies the ESI ping health check configuration. Use the [show esi ping](#) command to show ESI ping information.

Parameter	Description
<ping_inst>	Specifies the ping health check configuration.
frequency <frequency_inst>	Specifies the ping frequency, in seconds. 1-65535 seconds 5 seconds
no	Negates any configured parameter.
retry-count <retry-count_inst>	Specifies the ping retry count. 1-65535 2
timeout <timeout_inst>	Specifies the ping timeout, in seconds. 1-65535 seconds 2 seconds

Example

The following command specifies the ping health check attributes.

```
(host) [md] (config) #esi ping default
frequency 5
retry-count 2
timeout 2
```

Related Commands

Command	Description
<code>show esi ping</code>	Displays ESI ping information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

esi server

```
esi server <server_inst>
  dport <tcp-udp-port>
  mode {bridge|nat|route}
  no
  trusted-ip-addr <trusted-ip-addr_inst> [health-check]
  trusted-port <slot/port> |
  untrusted-ip-port <untrusted-ip-addr_inst> [health-check]
  untrusted-port <slot/port>
```

Description

This command configures an ESI server.

Parameter	Description
<server_inst>	Specifies the ESI server configuration.
dport <tcp-udp-port>	Specifies the NAT destination TCP or UDP port.
mode	Specifies the ESI server mode of operation: <ul style="list-style-type: none">▪ bridge: ESI server operates as a transparent bridge▪ nat: NAT destination addresses for the ESI server▪ route: ESI server operates as a router
no	Negates any configured parameter.
trusted-ip-addr <trusted-ip-addr_inst>	Specifies the server IP address on the trusted network. As an option, you can also enable a health check on the specified address
trusted-port <slot/port>	Specifies the port connected to the trusted side of the ESI server. The interface must be in <slot>/<port> format.
untrusted-ip-addr <untrusted-ip-addr_inst>	Specifies the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address
untrusted-port <slot/port>	Specifies the port connected to the untrusted side of the ESI server. The interface must be in <slot>/<port> format.

Example

The following command specifies the ESI server attributes:

```
(host) [md] (config) #esi server forti_1
mode route
```

```
trusted-ip-addr 10.168.172.3
untrusted-ip-addr 10.168.171.3
```

Related Commands

Command	Description
show esi servers	Displays configuration information for ESI servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

est

```
est profile <profile_name>
  arbitrary-label <arbitrary-label>
  arbitrary-label-enrolment <arbitrary-label-enrolment>
  arbitrary-label-reenrolment <arbitrary-label-reenrolment>
  challenge-password <challenge-password>
  clone <source>
  csr_attribute <attribute-type>
  organizational-unit-name <name>
  server-host <server-host>
  server-port <server-port>
  trustanchor-name <trustanchor-name>
  username <username>
  password <password>
  no..
```

Description

This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment. Use this command to configure an EST profile on the controller.

Parameter	Description
profile <profile_name>	Denotes the profile name of the EST profile.
arbitrary-label <arbitrary-label>	Sets an arbitrary label for the EST URI to distinguish it from the other EST profiles running on the EST server.
arbitrary-label-enrolment <arbitrary-label-enrolment>	Sets an arbitrary enrollment label for EST URI.
arbitrary-label-reenrolment <arbitrary-label-reenrolment>	Sets an arbitrary re-enrollment label for EST URI.
challenge-password <challenge-password>	Sets a challenge password used in CSR.
clone <source>	Name of an existing EST profile from which parameter values are copied.

Parameter	Description
csr_attribute	Configures the csr attribute type. Default is 2048 bit RSA with SHA 256 digest.
organizational-unit-name <name>	Sets the organizational unit name. String length: 1 to 63
server-host <server-host>	Denotes the IPv4 address or the hostname of the EST server.
server-port <server-port>	Indicates the port value of the EST server. The default value is 443.
trustanchor-name <trustanchor-name>	Denotes the server's trustanchor.
username <username>	Sets an username for the EST Client.
password <password>	Sets a password for the EST Client.
no..	Deletes the configuration.

Example

The following command configures an EST profile:

```
(host) [mynode] (config)# est profile est-new
(host) [mynode] (est profile "est-new" )# server-host 10.15.33.232
(host) [mynode] (est profile "est-new" )# server-port 443
(host) [mynode] (est profile "est-new" )# arbitrary-label /ca:2
(host) [mynode] (est profile "est-new" )# arbitrary-label-enrolment /ca:7
(host) [mynode] (est profile "est-new" )# arbitrary-label-reenrolment /ca:7
(host) [mynode] (est profile "est-new" )# csr_attribute ECDSAprime384r1_
with_SHA384
(host) [mynode] (est profile "est-new" )# challenge-password pass123
(host) [mynode] (est profile "est-new" )# trustanchor-name trust456
```

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>csr_attribute</code> parameter was introduced.
ArubaOS 8.6.0.0	The following parameters were introduced: <ul style="list-style-type: none"> ▪ <code>arbitraty label enrolment</code> ▪ <code>arbitrart label reenrolment</code> ▪ <code>organizational unit name</code> ▪ <code>username/password</code>
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode and config submode on Mobility Conductor.

est-activate

```
est-activate <profile_name>
```

Description

This command is used to activate an existing EST profile on the controller or the AP. Use this command to activate an EST profile on the controller or the AP.

Parameter	Description
<profile_name>	Denotes the profile name of the EST profile to be activated.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

execute

```
execute chat_script <chat_script_cmd>
```

Description

This command executes the specified CLI command.

Parameter	Description
chat_script <chat_script_cmd>	Specify the custom or pre_set chat command to be executed.

Example

This command executes the chat command modem-em12-status.

```
(host-md) #execute chat_script modem-em12-status
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

execute-cli

```
execute-cli  
  remote-ip-addr {<ip-addr> | <ip6-addr>}  
  command <cmd_str>
```

Description

This command executes the specified CLI command on the remote device.

Parameter	Description
remote-ip-addr {<ip-addr> <ip6-addr>}	Specify the IP address of the managed device on which the command is to be executed.
command <cmd_str>	Specify the full valid command string to be executed on the remote managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

exit

exit

Description

This command exits the current CLI mode.

Upon entering this command in a configuration submode, you are returned to the configuration mode. Upon entering this command in configuration mode, you are returned to the enable mode. Upon entering this command in enable mode, you are returned to the user login.

Example

The following sequence of `exit` commands return the user from the interface configuration submode to the user login:

```
(host) [mynode] (config-if) #exit
(host) [mynode] (config) #exit
(host) [mynode] #exit
User:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

export

```
export gap-db <filename>
```

Description

This command exports the global AP database to the specified file. This command is intended for system troubleshooting. You should run this command only when directed to do so by an Aruba support representative.

The global AP database resides on Mobility Conductor and contains information about known APs on all managed devices in the system. You can view the contents of the global AP database with the `show ap database` command.

Parameter	Description
<filename>	Name of the file to which the global AP database is exported.

Example

The following command exports the global AP database to a file:

```
(host) [mynode] #export gap-db global-ap-db
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

extifmgr

extifmgr verbose-log

Description

This command enables debug logs for the external interface manager process in Mobility Conductor.

The external interface manager process communicates with third-party applications like Palo Alto Networks firewall. Execute this command under the supervision of Aruba TAC.

Example

The following command exports the global AP database to a file:

```
(host) [mynode] #extifmgr verbose-log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

file syncing profile

```
file syncing profile
  file-syncing-enable
  no
  sync-time <sync-time>
```

Description

This command allows the user to configure the file syncing profile. This command enables or disables the file syncing. Additionally, the time between syncs can be configured as part of the file syncing profile.

Parameter	Description
file-syncing-enable	Enables file syncing on the managed device. Enabled
no	Negates any configured parameter.
sync-time <sync-time>	Configures the time between file syncs, in minutes. 30 -180 minutes 30 minutes

Example

The following example shows how to enable the file syncing:

```
(host) [md] (config) #file syncing profile
(host) (File syncing profile) #file-syncing-enable
```

Related Commands

Command	Description
show file syncing profile	Displays the configured file syncing profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

fips

fips [disable|enable]



This command applies only to the FIPS version of ArubaOS.

Description

This command enables and disables the FIPS mode of operation.

Parameter	Description
enable	Enables the FIPS mode of operation.
disable	Disables the FIPS mode of operation.

Example

The following example shows how to enable the FIPS mode of operation:

```
(host) [md] #fips enable
```

Related Commands

Command	Description
show fips	Indicates if FIPS is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Available in the base operating system.	Enable mode on Mobility Conductor.

firewall

```
firewall
  allow-tri-session
  amsdu
  app-perf-monitoring
  attack-rate
    arp <1-16384> {blacklist/denylist|drop}
    cp <1-16384>
    grat-arp <1-16384> {blacklist/denylist|drop}
    ping <1-16384>
    session <1-16384>
    tcp-syn <1-16384>

  bwcontracts-subnet-broadcast
  cp-bandwidth-contract
  debug-route
  deny-inter-user-bridging
  deny-inter-user-traffic
  deny-needfrag-df-gre-xmit-icmp
  deny-needfrag-df-gre
  deny-needfrag-df-ipsec
  deny-needfrag-gre-xmit-icmp
  deny-needfrag-gre
  deny-source-routing
  dhcp-perf monitoring
  disable-ftp-server
  dpi
  drop-ip-fragments
  enable-bridging
  enable-gre-inner-pkt-frag
  enable-per-packet-logging
  enable-port-packet-drop-logging
  enable-stateful-icmp
  enforce-tcp-handshake
  enforce-tcp-sequence
  gre-call-id-processing
  imm-fb
  ip-classification
  ipsec-mark-mgmt-frames
  jumbo
  local-valid-users
  log-icmp-error
  macast-red maxp-inv <maxp-inv> min-th <minimum-threshold> max-th <maximum
  threshold>
  optimize-dad-frames
  prevent-dhcp-exhaustion
  prohibit-arp-spoofing
  prohibit-ip-spoofing
  prohibit-ip-spoofing-all
  prohibit-rst-replay
  prohibit-rc-update
  public-access
  session-idle-timeout <seconds>
```



```

session-spread
session-tunnel-fib
shape-mcast
stall-crash
track-spoof
voip-qos-trusted
voip-wmm-content-enforcement
web-cc
web-cc-cache-miss-drop
wireless-bridge-aging

```

Description

This command configures global firewall options on the managed device.

Parameter	Description
allow-tri-session	Allows three-way session when performing destination NAT. This option should be enabled when the managed device is not the default gateway for wireless clients and the default gateway is behind the managed device. This option is typically used for captive portal configuration. Disabled
amsdu	Aggregated Medium Access Control Service Data Units (AMSDU) packets are dropped if this option is enabled. Disabled
app-perf-monitoring	Enables app performance monitoring. This parameter is used to measure the time taken for an application to respond.
<pre> attack-rate arp <1-16384> {blacklist/denylist drop} cp <1-16384> grat-arp <1-16384> {blacklist/denylist drop} ping <1-16384> session <1-16384> tcp-syn <1-16384> </pre>	<p>Sets rates which, if exceeded, can indicate a denial of service attack.</p> <ul style="list-style-type: none"> arp: Monitor/police ARP attack (non Gratuitous ARP). 100 cp: Monitor/police control processor attack. grat-arp: Monitor/police Gratuitous ARP attack. 50 ping: Monitor ping attack. session: Monitor IP session attack. tcp-syn: Monitor TCP SYN attack.

Parameter	Description
	1-16384 is the number of requests per 30 seconds.
<code>bwcontracts-subnet-broadcast</code>	Applies bw contracts to local subnet broadcast traffic.
<code>cp-bandwidth-contract</code>	Configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.
<code>debug-route</code>	Enable route or route-cache specific IP tracing in datapath.
<code>disable</code>	Disable route or route-cache debugging in datapath
<code>ipv4 <ipv4-addr></code>	Specify IPv4 route or route-cache address.
<code>ipv6 <ipv6-addr></code>	Specify IPv6 route or route-cache address.
<code>deny-inter-user-bridging</code>	Prevents the forwarding of Layer2 traffic between wired or wireless users. You can configure user role policies that prevent Layer3 traffic between users or networks but this does not block Layer2 traffic. This option can be used to prevent traffic, such as Appletalk or IPX from being forwarded. If enabled, traffic (all non-IP traffic) to untrusted port or tunnel is also blocked. Disabled
<code>deny-inter-user-traffic</code>	Denies downstream traffic between users in a wireless network (untrusted users) by disallowing layer2 and layer3 traffic. This parameter does not depend on the <code>deny-inter-user-bridging</code> parameter being enabled or disabled. Disabled
<code>deny-needfrag-df-gre-xmit-icmp</code>	Drops IP packets with DF bit set when packet length is greater than GRE tunnel MTU and an ICMP error message is sent. Disabled

Parameter	Description
deny-needfrag-df-gre	Drops IP packets with DF bit set when packet length is greater than GRE tunnel MTU and an ICMP error message is not sent. disabled
deny-needfrag-df-ipsec	Drops IP packets with DF bit set when packet length is greater than IPsec tunnel MTU and an ICMP error message is sent. Enabled
deny-needfrag-gre-xmit-icmp	Drops IP packets when packet length is greater than GRE tunnel MTU and an ICMP error message is sent. Disabled
deny-needfrag-gre	Drops IP packets when packet length is greater than GRE tunnel MTU and an ICMP error message is not sent. Disabled
deny-source-routing	Disallows forwarding of IP frames with source routing with the source routing options set. Disabled
dhcp-perf monitoring	Enables DHCP performance monitoring. This parameter is used to measure the time taken for a DHCP exchange. Disabled
disable-ftp-server	Disables the FTP server on the managed device. Enabling this option prevents FTP transfers. Enabling this option could cause APs to not boot up. You should not enable this option unless instructed to do so by an Aruba representative. disabled
dpi	Enables DPI. Disabled
drop-ip-fragments	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Aruba representative.

Parameter	Description
	Disabled
enable-bridging	Enables bridging when the managed device is in factory default. Disabled
enable-gre-inner-pkt-frag	Enables fragmenting inner IP frames when packet length is greater than GRE tunnel MTU. Disabled
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Aruba representative, as doing so may create unnecessary overhead on the managed device. Disabled
enable-port-packet-drop-logging	Enables port packet logging. If enabled, the dropped frames are logged. Disabled
enable-stateful-icmp	Enables stateful ICMP processing. This parameter create sessions for ICMP errors and denies unidirectional replies. Disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network. Disabled
enforce-tcp-sequence	Enforces the TCP sequence numbers for all packets. Disabled

Parameter	Description
<code>gre-call-id-processing</code>	Creates a unique state for each PPTP tunnel. Do not enable this option unless instructed to do so by a technical support representative. Disabled
<code>imm-fb</code>	Immediately free buffers on managed device. Do not enable this option unless instructed to do so by a technical support representative. Disabled
<code>ip-classification</code>	Enables IP reputation / geolocation classification.
<code>ipsec-mark-mgmt-frames</code>	This parameter marks management frames.
<code>jumbo</code>	Enables jumbo frames processing. Disabled
<code>local-valid-users</code>	Adds only IP addresses, which belong to a local subnet, to the user-table. Disabled
<code>log-icmp-error</code>	Logs received ICMP errors. You should not enable this option unless instructed to do so by a customer support representative. Disabled
<code>macast-red</code>	Configures multicast random drop parameters. Disabled
<code>maxp-inv <maxp-inv></code>	Inverse mark probability instance. 1-255
<code>min-th <minimum threshold></code>	Configures minimum threshold. 1-99
<code>max-th <maximum threshold></code>	Configures maximum threshold. 1-99
<code>optimize-dad-frames</code>	Reduce flooding of IPv4 Gratuitous ARPs/IPv6 Duplicate Address Detection frames onto wireless clients. Enabled

Parameter	Description
prevent-dhcp-exhaustion	<p>Enable check for DHCP client hardware address against the packet source MAC address. This command checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.</p> <p>Disabled</p>
prohibit-arp-spoofing	<p>Detects and prohibits arp spoofing. When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.</p> <p>Disabled</p>
prohibit-ip-spoofing	<p>Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.</p> <p>Enabled in IPv4, disabled in IPv6</p>
prohibit-ip-spoofing-all	<p>Detects ARP spoofing, when an intruder sends ARP using the IP and MAC addresses of a known user. When this option is enabled, additional check for the user route cache entry is performed. If the route cache entry is not found or if found, but the route cache entry MAC does not match with the sender MAC in ARP frame, then, the frame is marked as spoof. The IP spoofing attacks are logged and an SNMP trap is sent. If the Prohibit IP Spoofing option is enabled, the controller denies all the traffic from the client using an IP address that is used by another client that has an entry in the user table. This option does not allow multiple MAC addresses to use the same IP address.</p> <p>Disabled</p>
prohibit-rc-update	<p>This option prohibits route-cache update on user add.</p>

Parameter	Description
	Disabled
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Aruba representative. Disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Aruba representative. 16-300 16
session-spread	Enables counter CPU to perform encryption. Applicable to 7200 Series controllers only Disabled
session-tunnel-fib	Enable session tunnel-based forwarding. NOTE: Best practices is to enable this parameter only during maintenance window or off-peak production hours. On the M3, this parameter only enables tunnel-based forwarding, as session-based forwarding does not apply to this platform.
shape-mcast	Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used. Disabled
stall-crash	Triggers datapath crash on stall detection. Applies to the to 7200 Series managed device only. Enabled
track-spoof	If enabled, detects spoof in datapath. Disabled

Parameter	Description
voip-qos-trusted	<p>Prioritizes the RTP traffic based on the DSCP value set by the end user device.</p> <p>NOTE: On enabling, all UCC based ALGs will be disabled.</p> <p>Disabled</p>
voip-wmm-voip-content-enforcement	<p>If traffic to or from the user is inconsistent with the associated QoS policy for voice, the traffic is reclassified to best effort and data path counters incremented. This parameter requires the PEFNG license.</p> <p>Disabled</p>
web-cc	<p>Enables web content classification for all HTTP traffic. Once enabled, ArubaOS enforces ACLs and bandwidth policies associated with web content categories or reputation levels.</p> <p>NOTE: On enabling web-cc, the web-cc feature usage information will be sent to Aruba at every 7 days interval.</p> <p>Disabled</p>
web-cc-cache-miss-drop	<p>Issue this command to allow the managed device to drop any packets that do not match any web content category or reputation levels in the managed device's internal web content cache.</p> <p>Disabled</p>
wireless-bridge-aging	<p>Issue this command to prevent the aging of wireless client associated with AP.</p> <p>Enabled</p>

Example

The following command disallows forwarding of non-IP frames between users:

```
(host)[/md] (config) #firewall deny-inter-user-bridging
```


Related Commands

Command	Description
firewall cp	Creates whitelist/allolwlist session ACLs.
firewall cp-bandwidth-contract	Configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.
show firewall	Display a list of global firewall policies.

Command History

Release	Description
ArubaOS 8.11.0.0	Default rate added for <code>attack-rate arp</code> parameter.
ArubaOS 8.6.017 and 8.7.1.9	The deny-needfrag-df-ipsec parameter was introduced.
ArubaOS 8.6.0.9	The <code>prohibit-rc-update</code> parameter is added.
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.8.0.0	The <code>session-spread</code> and <code>prohibit-ip-spoof-all</code> parameters were added.
ArubaOS 8.7.0.0	The following parameters were introduced: <ul style="list-style-type: none">▪ <code>enable-gre-inner-pkt-frag</code>▪ <code>deny-needfrag-df-gre-xmit-icmp</code>▪ <code>deny-needfrag-df-gre</code>▪ <code>deny-needfrag-gre-xmit-icmp</code>▪ <code>deny-needfrag-gre</code>
ArubaOS 8.4.0.0	The <code>voip-qos-trusted</code> parameter was added.
ArubaOS 8.2.0.0	The <code>wireless-bridge-aging</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system except the <code>voip-wmm-voip-content-enforcement</code> parameter which requires the PEFNG license.	Config mode on Mobility Conductor.

firewall cp

```
firewall cp
  ipv4|ipv6 deny|permit <ip-addr><ip-mask>|any|{host <ip-addr>} proto{<ip-protocol-
  number> ports <start port number><end port
  number>}|ftp|http|https|icmp|snmp|ssh|telnet|tftp [bandwidth-contract
  <name>|<pbwm>]
  no...
```

Description

This command creates whitelist/allowlist session ACLs. Whitelist/allowlist ACLs consist of rules that explicitly permit or deny session traffic from being forwarded or not to the managed device. This prohibits traffic from being automatically forwarded to the managed device if it was not specifically denied in a blacklist/denylist. The maximum number of entries allowed in the whitelist/allowlist is 64.

Parameter	Description
ipv4 ipv6	Specifies ipv4 or ipv6.
deny permit	Specifies the entry to reject (deny) on the session ACL whitelist/allowlist. Specifies an entry that is allowed (permit) on the session ACL whitelist/allowlist.
<ip-addr><ip-mask>	IPv4/IPv6 source address and source mask.
any	Specifies any IPv4 or IPv6 source address.
host <ip-addr>	Indicates a specific IPv4 or IPv6 source address.
proto	Specify one of the following protocols used by the session traffic: <ul style="list-style-type: none">▪ ftp▪ http▪ https▪ icmp▪ scmp▪ ssh▪ telnet▪ tftp
bandwidth-contract <name>	Specify the name of a bandwidth contract. configures a bandwidth contract traffic rate, which can then be associated with a whitelist/allowlist session ACL

Parameter	Description
position <prio>	Specify filter position. Default is last position. 1 is first position.
IP protocol number	Specifies the IP protocol number that is permitted or denied. 1-255
start port	Specifies the starting port, in the port range, on which session traffic is running. 1-65535
end port	Specifies the last port, in the port range, on which session traffic is running. 1-65535
<pbwm>	Bandwidth rate in packets/seconds. 1-64000

Example

The following command creates a whitelist/allowlist ACL that allows on with the source address as 10.10.10.10 and the source mask as 2.2.2.2. The protocol is FTP and the bandwidth contract name is mycontract.

```
(host) [/md] (config-fw-cp) #ipv4 permit 10.10.10.10 2.2.2.2 proto ftp
bandwidth-contract name mycontract
```

The following command creates a whitelist/allowlist ACL entry that denies traffic using protocol 2 on port 5000 from being forwarded to the managed device:

```
(host) [/md] (config-fw-cp) #deny proto 6 ports 5000 6000
```

The following example configures a bandwidth contract named "cp-rate" with a rate of 100 pps.

```
(host) [/md] (config) #cp-bandwidth-contract cp-rate pps 100
```

Related Commands

Command	Description
show firewall-cp	Show Control Processor (CP) whitelist/allowlist ACL info.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> . All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

firewall-visibility

```
firewall-visibility
  blk-session
  feed <sort-by-bssid>
  no ...
```

Description

This command configures policy enforcement firewall visibility feature.

When you enable this feature, the **Firewall Monitoring** page on the **Dashboard** tab of the WebUI displays the summary of all sessions in the managed device aggregated by users, devices, destinations, applications, WLANs, and roles.

Parameter	Description
blk-session	Enables or disables blocked session logging and display.
feed <sort-by-bssid>	Enables or disables sorting of firewall visibility sessions based on the BSSID. Disabled

Example

The following command enables firewall visibility.

```
(host) [mynode] (config) #firewall-visibility
```

The following command enables grouping of firewall visibility sessions based on the same BSSID.

```
(host) [mynode] (config) #firewall-visibility feed sort-by-bssid
```

Related Commands

Command	Description
show firewall-visibility	Displays the policy enforcement firewall visibility process state and status information.

Command History

Release	Modification
ArubaOS 8.6.0.17 and 8.7.1.9	The feed <sort-by-bssid> parameter was introduced.
ArubaOS 8.10.0.0	The feed <sort-by-bssid> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Conductor.

firewall cp-bandwidth-contract

```
firewall cp-bandwidth-contract {arp-traffic|auth|ike <rate>|ippkt-err|l2-  
other|oflow|route|sessmirr|trusted-mcast|trusted-ucast  
|untrusted-mcast|untrusted-ucast | vrrp}
```

Description

This command configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.

Parameter	Description
arp-traffic	Specifies the arp traffic rate limit in packets per second. Is applied as a multiples of 32 in datapath. 1-65535 pps 976 pps
auth	Specifies the traffic rate limit that is forwarded to the authentication process. 1-65535 pps 976 pps
ike <rate>	Specifies the traffic rate limit from IKE to CP, in packets per second. 1-65535 pps 976 pps
ippkt-err	Specifies the rate limit error IP in packets per-second (Applied as a multiple of 32 in datapath) 1-65535 pps
l2-other	Specifies the traffic rate limit for L2 protocol and L2 special handling traffic. 1-65535 pps 976 pps
oflow mdns	Specifies the rate limit Openflow MDNS in packets per-second (Applied as a multiple of 32 in datapath) 1-65535 pps
route	Specifies the traffic rate limit that needs ARP requests. 1-65535 pps 976 pps

Parameter	Description
sessmirr	Specifies the session mirrored traffic forwarded to the managed device. 1-65535 pps 976 pps
trusted-mcast	Specifies the trusted multicast traffic rate limit. 1-65535 pps 1953 pps
trusted-ucast	Specifies the trusted unicast traffic rate limit. 1-98304 pps
untrusted-mcast	Specifies the untrusted multicast traffic rate limit. 1-65535 pps 1953 pps
untrusted-ucast	Specifies the untrusted unicast traffic rate limit. 1-65535 pps 9765 pps
vrrp	Specifies the rate limit of VRRP traffic routed to the control plane. 1-65535 pps 9765 pps

Example

The following command disallows forwarding of non-IP frames between users:

```
(host) [/md] (config) #firewall deny-inter-user-bridging
```

Related Commands

Command	Description
show firewall	Displays a list of global firewall policies and policy details.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Conductor.

fmn-trace

```
fmn-trace {start | stop}
```

Description

This command allows to start or stop recording of fmn traces.

Example

This command executes the chat command modem-em12-status.

```
(host-md) #execute chat_script modem-em12-status
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

geolocation

geolocation latitude <latitude> longitude <longitude>

Description

This command configures the geolocation of the device.

Parameter	Description
latitude <latitude>	Latitude of the device.
longitude <longitude>	Longitude of the device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Managed Device.

gsm trace

gsm trace channel <channel-name> application <application-name>

Description

This command enables tracing on cluster channel for stm application.

Parameter	Description
channel <channel-name>	This parameter includes the name of the channel.
application <application-name>	This parameter includes the name of the application.

Example

The following command enables tracing on cluster channel for stm application:

```
(host)[mm](config) #gsm trace channel cluster application stm
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

gateway health-check

```
gateway health-check  
  <interval> <threshold>
```

Description

This command configures the default gateway health check for the managed device.



The managed device is rebooted if the default gateway becomes unreachable.

Parameter	Description
<interval>	Health check interval. 30-600 seconds
<threshold>	Number of missed pings before the managed device reboots. 3-64

Example

The following command configures the default gateway health check with an interval of 60 seconds and threshold of 10:

```
(host) [/md] (config) #gateway health-check 60 10
```

Related Commands

Command	Description
show gateway health-check	Displays the current status of the gateway health check feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

gps

```
gpe service profile <profile-name>
  clone <source>
  dynamic-model
  enable
  no
```

Description

This command configures the GPS profile.

Parameter	Description
clone	Copy data from another GPS Service Profile.
<source>	Specify the name of GPS Service Profile to copy.
dynamic-model	Configure dynamic model of GPS.
airbornev1	Set the dynamic model of the GPS to airborne with 1g acceleration.
airbornev2	Set the dynamic model of the GPS to airborne with 2g acceleration.
airbornev4	Set the dynamic model of the GPS to airborne with 4g acceleration.
automotive	Set the dynamic model of the GPS to automotive.
bike	Set the dynamic model of the GPS to bike.
pedestrian	Set the dynamic model of the GPS to pedestrian.
portable	Set the dynamic model of the GPS to portable.
sea	Set the dynamic model of the GPS to sea.
stationary	Set the dynamic model of the GPS to stationary.
wrist	Set the dynamic model of the GPS to wrist-worn watch.
enable	Enable the GPS profile.
no	Disable the GPS profile.

Related Commands

Command	Description
show ap gps	Configure the GPS profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Managed Device.

guest-access-email

```
guest-access-email
  smtp-port <port>
  smtp-server
  no
```

Description

This command configures the SMTP server that is used to send guest emails. Guest emails are generated when a guest user account is created or when the Guest Provisioning user sends a guest user account email at a later time.

As part of the guest provisioning feature, the `guest-access-email` command allows you to set up the SMTP port and server that process guest provisioning email. This email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the **Guest Provisioning** page.

Parameter	Description
<code>smtp-port <port></code>	Identifies the SMTP port through which the guest-access email is sent. 1-65535 25
<code>smtp-server <IP-Address></code>	The SMTP server to which the guest-access email is sent.
<code>no</code>	Deletes the command configuration

Example

The following command creates a guest-access email profile and sends guest user email through SMTP server IP address 1.1.1.1 on port 25:

```
(host) [mynode] (config) #guest-access-email
(host) [mynode] (Guest-access Email Profile) #
(host) [mynode] (Guest-access Email Profile) #smtp-port 25
(host) [mynode] (Guest-access Email Profile) #smtp-server 1.1.1.1
```

Related Commands

Command	Description
show guest-access-email	Displays the guest access email profile configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ha

```
ha group-membership <group-membership>
ha group-profile <profile-name>
  clone <source>
  controller <ip> role {active|dual|standby}
  controller-v6 <ipv6> role {active|dual|standby}
  ha-on-bkup-lms
  heartbeat
  heartbeat-interval <heartbeat-interval>
  heartbeat-threshold <heartbeat-threshold>
  no
  over-subscription
  pre-shared-key <pre-shared-key>
  preemption
  state-sync
```

Description

This command configures the High Availability:Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

The High Availability:Fast Failover feature supports redundancy models with an active controller pair, or an active or standby deployment model with one backup controller supporting one or more active controllers. Each of these clusters of active and backup controllers comprises a high-availability group. Note that all active and backup controllers within a single high-availability group must be deployed in a single conductor-local topology. The High Availability:Fast Failover feature works across Layer-3 networks, so there is no need for a direct Layer-2 connection between controllers in a high-availability group.

By default, the active controller of an AP is the controller to which the AP first connects when it comes up. Other dual mode or standby mode controllers in the same High Availability group become potential standby controllers for that AP. This feature does not require that the active controller act as the configuration conductor for the local standby controller. A conductor controller in a conductor-local deployment can act as an active or a standby controller.

When the AP first connects to its active controller, that controller sends the AP the IP address of a standby controller, and the AP attempts to connect to the standby controller. If an AP that is part of a cluster with multiple backup controllers fails to connect to the first standby controller, the active controller will select a new standby controller for that AP, and the AP will attempt to connect to that standby controller. APs using control plane security establish an IPsec tunnel to their standby controller. APs that are not configured to use control plane security send clear, unencrypted information to the standby controller.

An AP will failover to its backup controller if it fails to contact its active controller through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

A controller using this feature can have one of three high-availability roles: **active**, **standby**, or **dual**. An active controller serves APs, but cannot act as a failover standby controller for any AP

except the ones that it serves as active. A standby controller acts as a failover backup controller, but cannot be configured as the primary controller for any AP. A dual controller can support both roles, and acts as the active controller for one set of APs, and also acts as a standby controller for another set of APs.

Parameter	Description
group-membership <group-membership>	Displays the high availability group in which the managed device or standby controller is a member.
ha group-profile <profile-name>	Creates a new high availability group, or define settings for an existing group.
clone <source>	Name of an existing high availability profile from which parameter values are copied.
controller <ip>	IPv4 address of a controller that should be added to the specified high availability group.
role	Assign one of the following roles to each controller in the high availability group. <ul style="list-style-type: none"> ▪ Active: controller is active and is serving APs. ▪ Dual: controller serves some APs and acts as a standby controller for other APs. ▪ Standby: controller does not serve APs, as only acts as a standby in case of failover.
controller-v6 <ipv6>	IPv6 address of a controller that should be added to the specified high availability group.
role	Assign one of the following roles to each controller in the high availability group. <ul style="list-style-type: none"> ▪ Active: controller is active and is serving APs. ▪ Dual: controller serves some APs and acts as a standby controller for other APs. ▪ Standby: controller does not serve APs, as only acts as a standby in case of failover.
ha-on-bkup-lms	This feature allows AP to honor the high availability configuration from bkup-lms and setup standby tunnel with standby controller, when AP reboots to bkup-lms.
heartbeat	The high availability inter-controller heartbeat feature allows for faster AP failover from an active controller to a standby controller, especially in situations where the active controller reboots or loses connectivity to the network.
heartbeat-interval <heartbeat-interval>	Enter a heartbeat interval in the Heartbeat Interval field to define how often inter-controller heartbeats are sent. 100-1000 ms

Parameter	Description
	100 ms
heartbeat-threshold <heartbeat-threshold>	Enter a heartbeat threshold in the Heartbeat Threshold field to define the number of heartbeats that must be missed before the APs are forced to fail over to the standby controller. 3-10 heartbeats 5 heartbeats
no	Negates or removes any configured parameter.
over-subscription	The standby controller over-subscription feature allows a standby controller to support connections to standby APs beyond the controller's original rated AP capacity. A controller acting as a standby controller can oversubscribe to standby APs by up to four times that controller's rated AP capacity, as long as the tunnels consumed the standby APs do not exceed the maximum tunnel capacity for that standby controller.
pre-shared-key <pre-shared-key>	Define a PSK to be used with the state synchronization feature. 8-32 characters
preemption	If you include this optional parameter to enable preemption, an AP that has failed over to a standby controller attempts to connect back to its original active controller once that controller is reachable again. When you enable this setting, the AP will wait for the time specified by the <code>lms-hold-down-period</code> parameter in the ap system-profile profile before the standby AP attempts to switch back to original controller.
state-sync	State synchronization improves failover performance by synchronizing PMK and Key cache values from the active controller to the standby controller, allowing clients to authenticate on the standby controller without repeating the complete 802.1X authentication process. NOTE: To use the state synchronization feature, configure a PSK with the pre-shared-key parameter.

Examples

The following commands configure a high availability group:

```
(host) [mynode] (config) #ha group-profile new
```

```
(host) [mynode] (HA group information "new") #controller 192.0.2.2 role active
(host) [mynode] (HA group information "new") #controller 192.0.2.3 role active
(host) [mynode] (HA group information "new") #controller 192.0.2.4 role standby
(host) [mynode] (HA group information "new") #preemption
```

Related Commands

Command	Description
show ha group	Displays HA profile settings.
show ha ap	Displays profile settings for APs using HA.
show ha heartbeat counters	Displays heartbeat statistics information for HA.
show ha oversubscription statistics	Displays oversubscription statistics information for HA.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

halt

halt

Description

This command gracefully stops all processes on the Mobility Conductor. You should issue this command before rebooting or shutting down to avoid interrupting processes.

Starting from ArubaOS 8.11.0.0, the **halt** command can be issued only from the **/mm** and **/mm/mynode** nodes of the Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.11.0.0	The command can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

help

help

Description

This command displays keyboard editing commands that allow you to make corrections or changes to the command without retyping.

You can also enter the question mark (?) to get various types of command help:

- When typed at the beginning of a line, the question mark lists all commands available in the current mode.
- When typed at the end of a command or abbreviation, the question mark lists possible commands that match.
- When typed in place of a parameter, the question mark lists available options.

Example

The following command displays help:

```
(host) [mynode] #help
HELP:
Special keys:
DEL, BS .... delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-T .... transpose previous character
Ctrl-P .... go to previous line in history buffer
Ctrl-N .... go to next line in history buffer
Ctrl-Z .... return to root command prompt
Tab, <SPACE> command-line completion
Exit .... go to next lower command prompt
?, Tab .... list choices
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
```

```
(e.g. 'show w?'.)
If on entering a 'tab', command-line completion is not possible
at that point, the behavior will be similar to entering a '?'.
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

hidehash

```
hidehash {disable | enable}
```

Description

This command controls the display of hashed passwords for management user in CLI.

Parameter	Description
disable	Hash code for management user password is displayed as it is.
enable	Hash code for management user password is displayed in encrypted format.

Example

```
(host) [mm] #hidehash disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Enable mode on the Mobility Conductor.

hostname

hostname <hostname>

Description

This command changes the hostname of the Mobility Conductor, standby controller, or managed device. The hostname is used as the default prompt. You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

Parameter	Description
<hostname>	The hostname of the Mobility Conductor, standby controller, or managed device. 1-63 characters

Example

The following example configures the Mobility Conductor hostname to "controller 1".

```
(host) [mm] (config) #hostname "controller 1"
```

Related Commands

Command	Description
show hostname	Displays the controller's hostname.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on the Mobility Conductor, standby controller, or managed device.

http-ping

http-ping <url>

Description

This command measures the latency of a webserver.

Parameter	Description
<url>	Specify the url to webserver.

Example

```
(host) [mm] #http-ping www.google.com

Pinging 'www.google.com'

Press 'q' to abort.
1> Reply: [0/] bytes=0 time=5ms Rate=0.00KB/sec
2> Reply: [0/] bytes=0 time=5ms Rate=0.00KB/sec
3> Reply: [0/] bytes=0 time=0ms Rate=0.00KB/sec
4> Reply: [0/] bytes=0 time=0ms Rate=0.00KB/sec
5> Reply: [0/] bytes=0 time=0ms Rate=0.00KB/sec

Ping Statistics for www.google.com
Packets: Sent : 5 Received : 0 Success Rate is 0 percent (0/5)
Approximate round trip time : max/avg/min = 5/2/0 ms
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on the Mobility Conductor, standby controller, or managed device.

iap del branch-key / iap del branch-name

iap del branch-key /iap del branch-name <brkey>

Description

This command removes a branch from the managed device based on the branch key.

Parameter	Description
branch-key <brkey>	Key for the branch, which is unique to each branch.

Example

```
(host) [mynode] #iap del branch-key  
b3c65c4d013836cf190566ca1afdf87c95350cffb1c782e463  
(host) [mynode] #iap del branch-name  
b3c65c4d013836cf190566ca1afdf87c95350cffb1c782e463
```

Related Command

Command	Description
show iap table	This command displays the branch details connected to the managed device.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command has been modified to <code>iap del branch-name</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

iapvpn-tunnel-trusted

iapvpn-tunnel-trusted

Description

This command is used to mark the IAP VPN tunnel as trusted tunnel.

Example

The following command marks IAP VPN tunnel as trusted tunnel.

```
(host) [mynode] (config) #iapvpn-tunnel-trusted
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

iap trusted-branch-db

```
iap trusted-branch-db
  add {mac-address <mac-address>}
  allow-all
  del {mac-address <mac-address>}
  del-all
```

Description

This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Parameter	Description
add	Configure an IAP trusted branch entry.
mac-address <mac-address>	MAC-address of the IAP.
allow-all	Configure all branches as trusted.
del	Delete an IAP trusted branch entry.
mac-address <mac-address>	MAC-address of the IAP.
del-all	Delete all trusted branch entries.

Example

The following command configures a specific IAP-VPN branch as trusted:

```
(host) [mynode] #iap trusted-branch-db add mac-address 01:01:0e:3e:4c:33
```

The following is the output of the above command:

```
Trusted branch added
```

This following command configures all IAP-VPN branches as trusted:

```
(host) [mynode] #iap trusted-branch-db allow-all
All IAP+VPN branches are trusted
```

Related Command

Command	Description
show iap detailed-table	This command displays the IAP trusted branch table.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config or Enable mode on Mobility Conductor.

iapvpn-backward-compatible

iapvpn-backward-compatible
no...

Description

This command is used to enable the older Instant APs to send register requests on the older HTTP port of 80.

In some scenarios, the controllers and Instant APs may not be upgraded simultaneously. However, if the Managed devices are upgraded first and if this command is not executed, all the register requests that are received on HTTP port 80 will be dropped by the managed device, resulting in service disruption. To prevent this from happening, the administrator has to enable this command as soon as the managed devices are upgraded to this version.

Parameter	Description
no	Disables IAP-VPN backward compatibility.

Example

The following command enables backward compatibility on older Instant APs:

```
(host) [mynode] (config) #iapvpn-backward-compatible
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ids ap-classification-rule

```
ids ap-classification-rule <rule-name>
  check-min-discovered-aps
  classify-to-type [neighbor|suspected-rogue]
  clone <source>
  conf-level-incr <conf-level-incr>
  discovered-ap-cnt <discovered-ap-cnt>
  match-ssids
  no
  snr-max <snr-max>
  snr-min <snr-min>
  ssid <ssid>
```

Description

This command configures the IDS AP classification rule profile.

AP classification rule configuration is performed only on the Mobility Conductor. If AMP is enabled via the mobility-manager command, then processing of the AP classification rules is disabled on Mobility Conductor. A rule is identified by its ASCII character string name (32 characters maximum). The AP classification rules must have one of the following specifications:

- SSID of the AP - Each rule can have up to six SSID parameters. If one or more SSIDs are specified in a rule, an option of whether to match any of the SSIDs, or to not match all of the SSIDs can be specified. The default is to check for a match operation.
- SNR of the AP- Each rule can have only one specification of the SNR. A minimum and maximum can be specified in each rule, and the specification is in SNR (db).
- Discovered-AP-Count or the number of APs that can see the AP- Each rule can have only one specification of the discovered-AP-count. Each rule can specify a minimum or maximum of the discovered-AP-count. The minimum or maximum operation must be specified if the discovered-AP-count is specified. The default setting is to check for the minimum discovered-AP-count.

Parameter	Description
<rule-name>	Name of the AP classification rule profile.
check-min-discovered-aps	Enables a rule check for the minimum number of APs. true
classify-to-type	Specifies the AP classification type as neighbor or suspected-rogue if the rule is matched. suspected-rogue
clone <source>	Copies data from another AP classification rule profile.

Parameter	Description
<code>conf-level-incr</code>	Increases the confidence level (in percentage) when the rule matches. 0-100 5
<code>discovered-ap-cnt</code> <code><discovered-ap-cnt></code>	The number of APs to be discovered. 0-100 0
<code>match-ssids</code>	Matches SSIDs. true false false
<code>no</code>	Negates any configured parameter.
<code>snr-max <snr-max></code>	Configures the maximum SNR value. 0-100 0
<code>snr-min <snr-min></code>	Configures the minimum SNR value. 0-100 0
<code>ssid <ssid></code>	Enter the keyword ssid followed by the SSID string to be matched or excluded

After you have created an AP classification rule, you must enable the rule by adding it to the IDS AP Matching Rules profile:

```
ids ap-rule-matching
rule-name <name>
```

Example

The following example configures the AP Configuration Rule Profile named "rule1", and then enables the rule by adding it to the IDS AP Matching Rules profile:

```
(host) [mynode] (config) #ids ap-classification-rule rule1
(host) [mynode] (IDS AP Classification Rule Profile "rule1") #check-min-
discovered-aps
(host) [mynode] (IDS AP Classification Rule Profile "rule1") #classify-to-
type neighbor
```

Related Command

Command	Description
show ids ap-classification-rule	Displays the IDS AP classification rule profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids ap-rule-matching

```
ids ap-rule-matching
  no
  rule-name <rule-name>
```

Description

This command configures the IDS active AP rules profile by enabling an AP classification rule. This command also activates an active AP rule created by the `ids ap-classification-rule` command. You must create the rule before you can activate it.

Parameter	Description
no	Negates any configured parameter.
rule-name <rule-name>	Name of the IDS AP classification rule to activate.

Example

```
(host) [mynode] (IDS Active AP Rules Profile) #rule-name rule2
```

Related Command

Command	Description
ids ap-classification-rule	Configures an IDS AP classification rule.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids dos-profile

```
ids dos-profile <profile-name>
  ap-flood-inc-time <ap-flood-inc-time>
  ap-flood-quiet-time <ap-flood-quiet-time>
  ap-flood-threshold <ap-flood-threshold>
  assoc-rate-thresholds <assoc-rate-thresholds>
  auth-rate-thresholds <auth-rate-thresholds>
  block-ack-dos-quiet-time <block-ack-dos-quiet-time>
  chopchop-quiet-time <chopchop-quiet-time>
  client-ht-40mhz-intol-quiet-time <client-ht-40mhz-intol-quiet-time>
  client-flood-inc-time <client-flood-inc-time>
  client-flood-quiet-time <client-flood-quiet-time>
  client-flood-threshold <client-flood-threshold>
  clone <source>
  cts-rate-quiet-time <cts-rate-quiet-time>
  cts-rate-threshold <cts-rate-threshold>
  cts-rate-time-interval <cts-rate-time-interval>
  deauth-rate-thresholds <deauth-rate-thresholds>
  detect-ap-flood
  detect-block-ack-dos
  detect-chopchop-attack
  detect-client-flood
  detect-cts-rate-anomaly
  detect-disconnect-sta
  detect-eap-rate-anomaly
  detect-fata-jack-attack
  detect-ghosttunnel-client-attack
  detect-ghosttunnel-server-attack
  detect-ht-40mhz-intolerance
  detect-invalid-address
  detect-malformed-association-request
  detect-malformed-auth-frame
  detect-malformed-htie
  detect-malformed-large-duration
  detect-omerta-attack
  detect-overflow-eapol-key
  detect-overflow-ie
  detect-power-save-dos-attack
  detect-rate-anomalies
  detect-rts-rate-anomaly
  detect-tkip-replay-attack
  detect-wpa-ft-attack
  disassoc-rate-thresholds <disassoc-rate-thresholds>
  disconnect-deauth-disassoc-threshold <disconnect-deauth-disassoc-threshold>
  disconnect-sta-assoc-resp-threshold <disconnect-sta-assoc-resp-threshold>
  disconnect-sta-quiet-time <disconnect-sta-quiet-time>
  eap-rate-quiet-time <eap-rate-quiet-time>
  eap-rate-threshold <eap-rate-threshold>
  eap-rate-time-interval <eap-rate-time-interval>
  fata-jack-quiet-time <fata-jack-quiet-time>
  ghosttunnel-client-attack-interval <ghosttunnel-client-attack-interval>
  ghosttunnel-client-attack-threshold <ghosttunnel-client-attack-threshold>
  ghosttunnel-client-quiet-time <ghosttunnel-client-quiet-time>
```

```

ghosttunnel-server-attack-interval <ghosttunnel-server-attack-interval>
ghosttunnel-server-attack-threshold <ghosttunnel-server-attack-threshold>
ghosttunnel-server-quiet-time <ghosttunnel-server-quiet-time>
invalid-address-combination-quiet-time <invalid-address-combination-quiet-time>
malformed-association-request-quiet-time <malformed-association-request-quiet-time>
malformed-auth-frame-quiet-time <malformed-auth-frame-quiet-time>
malformed-htie-quiet-time <malformed-htie-quiet-time>
malformed-large-duration-quiet-time <malformed-large-duration-quiet-time>
no
omerta-quiet-time <omerta-quiet-time>
omerta-threshold <omerta-threshold>
overflow-eapol-key-quiet-time <overflow-eapol-key-quiet-time>
overflow-ie-quiet-time <overflow-ie-quiet-time>
power-save-dos-min-frames <power-save-dos-min-frames>
power-save-dos-quiet-time <power-save-dos-quiet-time>
power-save-dos-threshold <power-save-dos-threshold>
probe-request-rate-thresholds <probe-request-rate-thresholds>
probe-response-rate-thresholds <probe-response-rate-thresholds>
rts-rate-quiet-time <rts-rate-quiet-time>
rts-rate-threshold <rts-rate-threshold>
rts-rate-time-interval <rts-rate-time-interval>
tkip-replay-quiet-time <tkip-replay-quiet-time>
wpa-ft-quiet-time
wpa-ft-threshold
wpa-ft-time-interval

```

Description

This command configures traffic anomalies for DoS attacks. DoS attacks are designed to prevent or inhibit legitimate clients from accessing the network. This includes blocking network access completely, degrading network service, and increasing processing load on clients and network equipment.

Parameter	Description
<profile-name>	Name of the IDS DoS profile. 1-63 characters "default"
ap-flood-inc-time <ap-flood-inc-time>	Time, in seconds, during which the AP count is over the threshold (AP flood). 0-36000 seconds 3600 seconds
ap-flood-quiet-time <ap-flood-quiet-time>	After an alarm has been triggered by an AP flood, the time, in seconds, that must elapse before an identical alarm may be triggered. 60-360000 seconds

Parameter	Description
	900 seconds
ap-flood-threshold <ap-flood-threshold>	Threshold for the number of spurious APs in the system. 0-100,000 50
assoc-rate-thresholds <assoc-rate-thresholds>	Rate threshold for associate request frames.
auth-rate-thresholds <auth-rate-thresholds>	Rate threshold for authenticate frames.
block-ack-dos-quiet-time <block-ack-dos-quiet-time>	Time to wait, in seconds, after detecting an attempt to reset the receive window using a forged block ACK add. 60-360000 seconds 900 seconds
chopchop-quiet-time <chopchop-quiet-time>	Time to wait, in seconds, after detecting a ChopChop attack after which the check can be resumed. 60-360000 seconds 900 seconds
client-ht-40mhz-intol-quiet-time <client-ht-40mhz-intol-quiet=time>	Quiet time (when to stop reporting intolerant STAs if they have not been detected), in seconds, for detection of 802.11n 40 MHz intolerance setting. 60-360000 seconds 900 seconds
client-flood-inc-time <client-flood-inc-time>	Number of consecutive seconds over which the client count is more than the threshold. 0-36000 seconds 3 seconds
client-flood-quiet-time <client-flood-quiet-time>	Time to wait, in seconds, after detecting a client flood before continuing the check. 60-360000 seconds 900 seconds
client-flood-threshold <client-flood-threshold>	Threshold for the number of spurious clients in the system. 0-100000

Parameter	Description
	150
clone <source>	Copies data from another IDS Denial Of Service Profile.
cts-rate-quiet-time <cts-rate-quiet-time>	Time to wait, in seconds, after detecting a CTS rate anomaly after which the check can be resumed. 60-360000 seconds 900 seconds
cts-rate-threshold <cts-rate-threshold>	Number of CTS control packets over the time interval that constitutes an anomaly. 0-100000 5000
cts-rate-time-interval <cts-rate-time-interval>	Time interval, in seconds, over which the packet count should be checked. 1-120 seconds 5 seconds
deauth-rate-thresholds <deauth-rate-thresholds>	Rate threshold for deauthenticate frames.
detect-ap-flood	Enables or disables detection of AP flood attacks. disabled
detect-block-ack-dos	Enables or disables detection of attempts to reset traffic receive windows using forged Block ACK Add messages. enabled
detect-chopchop-attack	Enables or disables detection of ChopChop attacks. disabled
detect-client-flood	Enables or disables detection of client flood attacks. disabled
detect-cts-rate-anomaly	Enables or disables detection of CTS rate anomalies. disabled

Parameter	Description
detect-disconnect-sta	<p>In a station disconnection attack, an attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association.</p> <p>Use this command to enable the detection of disconnect station attack.</p> <p>enabled</p>
detect-eap-rate-anomaly	<p>Enables or disables detection of the EAP handshake rate anomaly.</p> <p>disabled</p>
detect-fata-jack-attack	<p>Enables or disables detection of FATA-Jack attacks.</p> <p>enabled</p>
detect-ghosttunnel-client-attack	<p>Enables or disables detection of ghost tunnel client attacks.</p> <p>disabled</p>
detect-ghosttunnel-server-attack	<p>Enables or disables detection of ghost tunnel server attacks.</p> <p>disabled</p>
detect-ht-40mhz-intolerance	<p>Enables or disables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.</p> <p>disabled</p>
detect-invalid-address	<p>Enables or disables detection of invalid address combinations.</p> <p>disabled</p>
detect-malformed-association-request	<p>Enables or disables detection of malformed association requests.</p> <p>disabled</p>
detect-malformed-auth-frame	<p>Enables or disables detection of malformed authentication frames.</p> <p>disabled</p>
detect-malformed-htie	<p>Enables or disables detection of malformed HT IE.</p> <p>disabled</p>

Parameter	Description
detect-malformed-large-duration	Enables or disables detection of unusually large durations in frames. enabled
detect-omerta-attack	Enables or disables detection of Omerta attacks. enabled
detect-overflow-eapol-key	Enables or disables detection of overflow EAPOL key requests. disabled
detect-overflow-ie	Enables or disables detection of overflow IEs. disabled
detect-power-save-dos-attack	Enables or disables detection of Power Save DoS attacks. enabled
detect-rate-anomalies	Enables or disables detection of rate anomalies. disabled
detect-rts-rate-anomaly	Enables or disables detection of RTS rate anomalies. disabled
detect-tkip-replay-attack	Enables or disables detection of TKIP replay attacks. disabled
detect-wpa-ft-attack	Enables or disables detection of WPA FT attacks. disabled
disassoc-rate-thresholds <disassoc-rate-thresholds>	Rate threshold for disassociate frames.
disconnect-deauth-disassoc-threshold <disconnect-deauth-disassoc-threshold>	Number of deauthentication or disassociation frames seen in an interval of 10 seconds. 1-50 8
disconnect-sta-assoc-resp-threshold <disconnect-sta-assoc-resp-threshold>	The number of successful Association Response or Reassociation response frames seen in an interval of 10 seconds.

Parameter	Description
	1-30 5
disconnect-sta-quiet-time <disconnect-sta-quiet-time>	After a station disconnection attack is detected, the time, in seconds, that must elapse before the check can be resumed. 60-360000 seconds 900 seconds
eap-rate-quiet-time <eap-rate-quiet-time>	After an EAP rate anomaly alarm has been triggered, the time, in seconds, that must elapse before the check can be resumed. 60-360000 seconds 900 seconds
eap-rate-threshold <eap-rate-threshold>	Number of EAP handshakes that must be received within the EAP rate time interval to trigger an alarm. 0-100000 60
eap-rate-time-interval <eap-rate-time-interval>	Time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm. 1-120 seconds 3 seconds
fata-jack-quiet-time <fata-jack-quiet-time>	Time to wait, in seconds, after detecting a FATA-Jack attack after which the check can be resumed. 60-360000 seconds 900 seconds
ghosttunnel-client-attack-interval <ghosttunnel-client-attack-interval>	Time interval, in seconds, over which the packet count is checked. Default is 60 seconds. Maximum is 600 seconds.
ghosttunnel-client-attack-threshold <ghosttunnel-client-attack-threshold>	Number of probe request management packets for a fake AP over the time interval that constitutes a ghost tunnel attack. Default is 10. Maximum is 100000.
ghosttunnel-client-quiet-time <ghosttunnel-client-quiet-time>	Time to wait, in seconds, after detecting a ghost tunnel attack after which the check is resumed. Default is 900 seconds. Minimum is 60 seconds.

Parameter	Description
ghosttunnel-server-attack-interval <ghosttunnel-server-attack-interval>	Time interval, in seconds, over which the packet count is checked. Default is 60 seconds. Maximum is 600 seconds.
ghosttunnel-server-attack-threshold <ghosttunnel-server-attack-threshold>	Number of beacon management packets for a fake AP over the time interval that constitutes a ghost tunnel attack. Default is 200. Maximum is 10000.
ghosttunnel-server-quiet-time <ghosttunnel-server-quiet-time>	Time to wait, in seconds, after detecting a ghost tunnel attack after which the check is resumed. Default is 900 seconds. Minimum is 60 seconds.
invalid-address-combination-quiet-time <invalid-address-combination-quiet-time>	Time to wait, in seconds, after detecting an invalid address combination after which the check can be resumed. 60-360000 seconds 900 seconds
malformed-association-request-quiet-time <malformed-association-request-quiet-time>	Time to wait, in seconds, after detecting a malformed association request after which the check can be resumed. 60-360000 seconds 900 seconds
malformed-auth-frame-quiet-time <malformed-auth-frame-quiet-time>	Time to wait, in seconds, after detecting a malformed authentication frame after which the check can be resumed. 60-360000 seconds 900 seconds
malformed-htie-quiet-time <malformed-htie-quiet-time>	Time to wait, in seconds, after detecting a malformed HT IE after which the check can be resumed. 60-360000 seconds 900 seconds
malformed-large-duration-quiet-time <malformed-large-duration-quiet-time>	Time to wait, in seconds, after detecting a large duration for a frame after which the check can be resumed. 60-360000 seconds 900 seconds
no	Negates any configured parameter.

Parameter	Description
omerta-quiet-time <omerta-quiet-time>	Time to wait, in seconds, after detecting an Omerta attack after which the check can be resumed. 60-360000 seconds 900 seconds
omerta-threshold <omerta-threshold>	The Disassociation packets received by a station as a percentage of the number of data packets sent, in an interval of 10 seconds. 1-100 10%
overflow-eapol-key-quiet-time <overflow-eapol-key-quiet-time>	Time to wait, in seconds, after detecting a overflow EAPOL key request after which the check can be resumed. 60-360000 seconds 900 seconds
overflow-ie-quiet-time <overflow-ie-quiet-time>	Time to wait, in seconds, after detecting a overflow IE after which the check can be resumed. 60-360000 seconds 900 seconds
power-save-dos-min-frames <power-save-dos-min-frames>	The minimum number of Power Management OFF packets that are required to be seen from a station, in intervals of 10 second, in order for the Power Save DoS check to be done. 1-1000 120
power-save-dos-quiet-time <power-save-dos-quiet-time>	Time to wait, in seconds, after detecting a Power Save DoS attack after which the check can be resumed. 60-360000 seconds 900 seconds
power-save-dos-threshold <power-save-dos-threshold>	The Power Management ON packets sent by a station as a percentage of the Power Management OFF packets sent, in intervals of 10 second, which will trigger this event. 1- 100% 80%

Parameter	Description
probe-request-rate-thresholds <probe-request-rate-thresholds>	Rate threshold for probe request frames.
probe-response-rate-thresholds <probe-response-rate-thresholds>	Rate threshold for probe response frames.
rts-rate-quiet-time <rts-rate-quiet-time>	Time to wait, in seconds, after detecting an RTS rate anomaly after which the check can be resumed. 60-360000 seconds 900 seconds
rts-rate-threshold <rts-rate-threshold>	Number of RTS control packets over the time interval that constitutes an anomaly. 0-100000 5000
rts-rate-time-interval <rts-rate-time-interval>	Time interval, in seconds, over which the packet count should be checked. 1-120 seconds 5 seconds
tkip-replay-quiet-time <tkip-replay-quiet-time>	Time to wait, in seconds, after detecting a TKIP replay attack after which the check can be resumed. 60-360000 seconds 900 seconds
wpa-ft-quiet-time <wpa-ft-quiet-time>	Time to wait, in seconds, after detecting a WPA FT attack after which the check can be resumed. 60-360000 seconds 900 seconds
wpa-ft-threshold <wpa-ft-threshold>	Number of reassociation management packets for a particular client over the time interval that constitutes a WPA FT attack. 0-100000 45
wpa-ft-time-interval <wpa-ft-time-interval>	Time interval, in seconds, over which the packet count should be checked. 1-120 seconds 60 seconds

Example

The following command enables a detection in the DoS profile named "floor2":

```
(host) [mynode] (config) #ids dos-profile floor2
(host) [mynode] (IDS Denial Of Service Profile "floor2") detect-ap-flood
```

Related Command

Command	Description
show ids dos-profile	Displays the IDS DoS profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The following parameters were added: <ul style="list-style-type: none">detect-ghosttunnel-client-attackdetect-ghosttunnel-server-attackghosttunnel-client-attack-intervalghosttunnel-client-attack-thresholdghosttunnel-client-quiet-timeghosttunnel-server-attack-intervalghosttunnel-server-attack-thresholdghosttunnel-server-quiet-time
ArubaOS 8.6.0.0	Removed spoofed deauth blacklist parameter.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none">detect-wpa-ft-attackwpa-ft-quiet-timewpa-ft-thresholdwpa-ft-time-interval
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids general-profile

```
ids general-profile <profile-name>
  adhoc-ap-inactivity-timeout
  adhoc-ap-max-unseen-timeout
  ap-inactivity-timeout <seconds>
  ap-max-unseen-timeout
  ap-nbr-msg
  ap-nbr-msg-interval <ap-nbr-msg-interval>
  client-detection-mode
  clone <profile>
  frame-types-for-rssi [all | ba | ctrl | dhigh | dlow | dnull | mgmt | pr]
  ids-events [logs-and-traps | logs-only | none | traps-only]
  max-monitored-aps <max-monitored-aps>
  max-monitored-devices <max-monitored-devices>
  max-unassociated-stations <max-unassociated-stations>
  min-pot-ap-beacon-rate <percent>
  min-pot-ap-monitor-time <seconds>
  mobility-manager-rtls
  mon-stats-update-interval
  no ...
  packet-snr-threshold <packet-snr-threshold>
  radio-info-ext-msg-interval
  send-adhoc-info-to-controller
  signature-quiet-time <seconds>
  sta-inactivity-timeout <seconds>
  sta-max-unseen-timeout <seconds>
  sta-rssi-msg
  sta-rssi-msg-interval <sta-rssi-msg-interval>
  stats-update-interval <seconds>
  unclass-ap-update
  unclass-device-update-interval
  unclass-sta-update
  valid-ap-max-unseen-time
  wired-containment
  wired-containment-ap-adj-mac
  wired-containment-susp-l3-rogue
  wireless-containment [deauth-only | none | tarpit-all-sta | tarpit-non-valid-sta]
  wireless-containment-deauth-reason <wireless-containment-deauth-reason>
  wireless-containment-debug
  wms-client-monitoring
```

Description

This command configures an IDS general profile and IDS profile attributes.



The feature for enabling wireless containment under the **IDS Unauthorized Device** profile and **IDS Impersonation** profile may be in violation of certain FCC regulatory statutes. To address this, a warning message will be issued each time the command is enabled through the CLI. The warning message will appear after the command is executed.

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. The name must be 1-63 characters. default
adhoc-ap-inactivity-timeout	Ad hoc (IBSS) AP inactivity timeout, in number of scans. 5-36000 seconds 5 seconds
adhoc-ap-max-unseen-timeout	Ageout time, in seconds, since ad hoc (IBSS) AP was last seen. 5-36000 seconds 5 seconds
ap-inactivity-timeout	Time, in seconds, after which an AP is aged out. 5-36000 seconds 5 seconds
ap-max-unseen-timeout	Ageout time, in seconds, since AP was last seen. 5-36000 seconds 600 seconds
ap-nbr-msg	Enables or disables AP neighbor messages. disabled
ap-nbr-msg-interval	Interval, in seconds, at which an AP delivers AP neighbor messages to the management server. 1-36000 seconds 1 second
client-detection-mode	NOTE: This setting applies only to detection of clients on scan channels in AP mode. Specify one of the following client detection mode: <ul style="list-style-type: none"> ▪ Normal: AP needs to detect only unidirectional traffic to discover the client. ▪ Strict: AP needs to detect bidirectional traffic to discover the client. This mode protects from invalid client entries being detected, but may increase the time taken to detect clients on scan channels.
clone	Name of an existing IDS general profile from which parameter values are copied.
frame-types-for-rssi	Select frame types to be used in AM RSSI calculation.

Parameter	Description
all ba ctrl dhigh dlow dnull mgmt pr	Frame types: <ul style="list-style-type: none"> ▪ all—All types of frames. This frame type overrides any other frame types. ▪ ba—Block ACK frame types. ▪ ctrl—All control frames except ACK. ▪ dhigh—Data frames more than 36 Mbps except null data frames. ▪ dlow—Data frames less than 36 Mbps except null data frames. ▪ dnull—Null data frames. ▪ mgmt—All management frames except probe request. ▪ pr—Probe request frames. <p>NOTE: Configure this parameter under the supervision of Aruba Technical Support.</p> <p>ba, ctrl, dlow, dnull, mgmt, pr</p>
ids-events logs-and-traps logs-only none traps-only]	Enables or disables IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch. <p>logs-and-traps</p>
max-monitored-aps	Maximum number of BSSIDs that can be monitored by a single AP. The actual upper limit may be smaller than the configured limit based on the available memory on different AP platforms. When set to 0, the default maximum value allowed for the AP platform will be applied. Display the maximum value with CLI command <code>show ap monitor debug profile-config ids-general</code> . <p>0</p>
max-monitored-devices	Maximum number of APs and stations that can be monitored. This number does not include stations that are not associated to any AP. Within this max value, the AP reserves a buffer for stations that are associated locally. Configure this parameter under the supervision of Aruba Technical Support. <p>1024-4096</p> <p>1024 or 4096, depending on the AP platform.</p>
max-unassociated-stations	Maximum number of unassociated stations. <p>NOTE: Configure this parameter under the supervision of Aruba Technical Support.</p> <p>256-4096</p>

Parameter	Description
	512
min-pot-ap-beacon-rate	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval. 0-100% 25%
min-pot-ap-monitor-time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP. 2-36000 seconds 2 seconds
mobility-manager-rtls	Enables or disables RTLS communication with the configured mobility-manager. disabled
mon-stats-update-interval	Time interval, in seconds, for the AP to update the switch with stats for monitored devices. 60-36000 seconds 60 seconds
no	Negates any configured parameter.
packet-snr-threshold	Sets the packet SNR threshold. All packets with SNR below this threshold is dropped from IDS and ARM processing. No packets are dropped if the threshold is set to 0. NOTE: Configure this parameter under the supervision of Aruba Technical Support. 0-90 dB 0
radio-info-ext-msg-interval	Specify interval in seconds for AP to deliver Radio Info Ext messages to the management servers. Minimum is 1 seconds. 300 seconds
send-adhoc-info-to-controller	Enables or disables sending ad hoc information to the controller from the AP. disabled
signature-quiet-time	After a signature match is detected, the time to wait, in seconds, to resume checking. 60-36000 seconds 900 seconds

Parameter	Description
<code>sta-inactivity-timeout</code>	Time, in seconds, after which a station is aged out. 30-36000 seconds 60 seconds
<code>sta-max-unseen-timeout</code>	Ageout time, in seconds, since station was last seen. 5-36000 seconds 600 seconds
<code>sta-rssi-msg</code>	Enables or disables station RSSI messages. disabled
<code>sta-rssi-msg-interval</code>	Interval, in seconds, at which the AP delivers station RSSI messages to the management server. 1-36000 1 second
<code>stats-update-interval</code>	Interval, in seconds, for the AP to update the controller with statistics. 60-36000 seconds 60 seconds
<code>unclass-ap-update</code>	Enables or disables classification updates for monitored APs. If this option is enabled, there is a decrease in the delay with which the devices are classified. disabled
<code>unclass-device-update-interval</code>	The time interval, in seconds, for the AP to send the WMS a list of unclassified APs and clients. 30-36000 seconds 60 seconds
<code>unclass-sta-update</code>	Enables or disables classification updates for monitored clients. If this option is enabled, there is a decrease in the delay with which the devices are classified. disabled
<code>wired-containment</code>	Enables or disables containment from the wired side. disabled
<code>wired-containment-ap-adj-mac</code>	Enables or disables wired containment of MACs offset by one from APs BSSID. disabled

Parameter	Description
wired- containment-susp-l3-rogue	<p>The basic wired containment feature enabled using the command contains layer-3 APs whose wired interface MAC addresses are either the same as (or one character off from) their BSSIDs. This feature can also identify and contain an AP with a preset wired MAC address that is completely different from the AP's BSSID if the MAC address that the AP provides to wireless clients as the 'gateway MAC' is offset by one character from its wired MAC address.</p> <p>NOTE: This feature requires that the following parameter in the ids general-profile is also enabled, and that the confidence level of the suspected rogue exceeds the level configured by the and parameters in the ids unauthorized-device-profile.</p>
wireless-containment	<p>Selects one of the following containment types from the wireless side:</p> <ul style="list-style-type: none"> ▪ death-only: Containment using deauthentication only. ▪ none: Disables wireless containment. ▪ tarpit-all-sta: Wireless containment by tarpit of all stations. ▪ tarpit-non-valid-sta: Wireless containment by tarpit of non-valid clients.
wireless-containment-death-reason	<p>Specify the death reason for containment from the wireless side. Range: 1 - 134. Default: 3</p>
wireless-containment-debug	<p>Enables or disables debugging of containment from the wireless side. Enabling this debug option will cause containment to not function properly.</p>
wms-client-monitoring	<p>Specify the WMS client monitoring level. This level controls which clients are monitored by WMS in the controller. The recommended value is 'all' to ensure full functionality of the system. Lowering the value will have a significant effect on features that rely on client classification or neighboring client signal strength. This setting should only be changed after consulting with TAC. all</p>

Example

The following commands enable containment in the general IDS profile:

```
(host) [mynode] (config) #ids general-profile floor7
(host) [mynode] (IDS General Profile "floor7") #wired-containment
(host) [mynode] (IDS General Profile "floor7") #wireless-containment tarpit-
all-sta
(host) [mynode] (IDS General Profile "floor7") #wireless-containment-debug
```

Command History

Release	Description
ArubaOS 8.9.0.0	The <code>wireless-containment-death-reason</code> parameter was introduced.
ArubaOS 8.5.0.0	The default value of <code>max-monitored-devices</code> parameter was modified to include both 1024 and 4096.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids impersonation-profile

```
ids impersonation-profile <profile-name>
  ap-spoofing-quiet-time <ap-spoofing-quiet-time>
  beacon-diff-threshold <beacon-diff-threshold>
  beacon-inc-wait-time <beacon-inc-wait-time >
  beacon-wrong-channel-quiet-time <beacon-wrong-channel-quiet-time>
  chan-based-mitm-quiet-time <chan-based-mitm-quiet-time>
  clone <source>
  detect-ap-impersonation
  detect-ap-spoofing
  detect-beacon-wrong-channel
  detect-chan-based-mitm
  detect-hotspotter
  hotspotter-quiet-time <hotspotter-quiet-time>
  no
  protect-ap-impersonation
```

Description

This command configures anomalies for impersonation attacks.

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. 1-63 characters "default"
ap-spoofing-quiet-time <ap-spoofing-quiet-time>	Time to wait, in seconds, after detecting AP Spoofing after which the check can be resumed. 60-360000 seconds 60 seconds
beacon-diff-threshold <beacon-diff-threshold>	Percentage increase, in beacon rates, that triggers an AP impersonation event. 0-100% 50%
beacon-inc-wait-time <beacon-inc-wait-time >	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated. 3 seconds
beacon-wrong-channel-quiet-time <beacon-wrong-channel-quiet-time>	Time to wait, in seconds, after detecting a beacon with the wrong channel after which the check can be resumed. 60-360000 seconds

Parameter	Description
	900 seconds
chan-based-mitm-quiet-time <chan-based-mitm-quiet-time>	Time to wait, in seconds, after detecting man-in-the-middle attack after which the check can be resumed. 60-360000 seconds 900 seconds
clone <source>	Name of an existing IDS impersonation profile from which parameter values are copied.
detect-ap-impersonation	Enables or disables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP or a neighboring AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack. enabled
detect-ap-spoofing	Enables or disables AP Spoofing detection. enabled
detect-beacon-wrong-channel	Enables or disables detection of beacons advertising the incorrect channel. disabled
detect-chan-based-mitm	Enables or disables channe-based man-in-the-middle attack detection. disabled
detect-hotspotter	Enables or disables detection of the Hotspotter attack to lure away valid clients. disabled
hotspotter-quiet-time <hotspotter-quiet-time>	Time to wait, in seconds, after detecting an attempt to use the Hotspotter tool against clients. 60-360000 seconds 900 seconds
no	Negates any configured parameter.
protect-ap-impersonation	When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack. disabled

Example

The following command enables detections in the impersonation profile:

```
(host) [mynode] (config) #ids impersonation-profile floor1
(host) [mynode] (IDS Impersonation Profile "floor1") #detect-beacon-wrong-channel
(host) [mynode] (IDS Impersonation Profile "floor1") #detect-ap-impersonation
```

Related Command

Command	Description
show ids impersonation-profile	Displays the IDS impersonation profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none">■ chan-based-mitm-quiet-time■ detect-chan-based-mitm
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids management-profile

```
ids management-profile
  event-correlation [logs-and-traps|logs-only|none|traps-only]
  event-correlation-quiet-time <event-correlation-quiet-time>
```

Description

This command configures the IDS WMS management profile and manages the events correlation for IDS event traps and syslogs (logs).

Parameter	Description
event-correlation	<p>Correlation mode for IDS event traps and syslogs (logs). Event correlation can be enabled with generation of correlated logs, traps, or both. To disable correlation, enter the keyword none.</p> <ul style="list-style-type: none">▪ logs-and-traps: Enables IDS event correlation with generation of correlated syslogs and traps.▪ logs-only: Enables IDS event correlation with generation of correlated syslogs only.▪ none: Disables IDS event correlation.▪ traps-only: Enables IDS event correlation with generation of correlated traps only. <p>logs-and-traps</p>
event-correlation-quiet-time	<p>Time to wait, in seconds, after generating a correlated event after which the event could be raised again. This only applies to events that are repeatedly raised by an AP.</p> <p>30-360000 seconds 900 seconds</p>

Example

```
(host) [mynode] (config) #ids management-profile
(host) [mynode] (IDS Management Profile) #event-correlation-quiet-time 30
(host) [mynode] (IDS Management Profile) #event-correlation logs-and-traps
```

Related Command

Command	Description
show ids management-profile	Displays the IDS WMS management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids profile

```
ids profile <profile-name>
  clone <source>
  dos-profile <profile-name>
  general-profile <profile-name>
  impersonation-profile <profile-name>
  no
  signature-matching-profile <profile-name>
  unauthorized-device-profile <profile-name>
```

Description

This command defines a set of IDS profiles that you can then apply to an AP group (with the `ap-group` command) or to a specific AP (with the `ap-name` command).

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. The name must be 1-63 characters. "default"
clone <source>	Name of an existing IDS profile from which parameter values are copied.
dos-profile <profile-name>	Name of a IDS DoS profile to be applied to the AP group or name. See ids dos-profile on page 682 . "default"
general-profile <profile-name>	Name of an IDS general profile to be applied to the AP group or name. See ids general-profile on page 694 . "default"
impersonation-profile <profile-name>	Name of an IDS impersonation profile to be applied to the AP group or name. See ids impersonation-profile on page 701 . "default"
no	Negates any configured parameter.
signature-matching-profile <profile-name>	Name of an IDS signature matching profile to be applied to the AP group or name. See ids signature-matching-profile on page 715 "default"
unauthorized-device-profile <profile-name>	Name of an IDS unauthorized device profile to be applied to the AP group or name. See ids unauthorized-device-profile on page 720 . "default"

Example

The following command defines a set of IDS profiles:

```
(host) [mynode] (config) #ids profile floor2
(host) [mynode] (IDS Profile "floor2") #dos-profile dos1
general-profile general1
impersonation-profile mitm1
signature-matching-profile sig1
unauthorized-device-profile unauth1
```

Related Commands

Command	Description
ids dos-profile	Configures an IDS DoS profile.
ids general-profile	Configures an IDS general profile.
ids impersonation-profile	Configures an IDS impersonation profile.
ids signature-matching-profile	Configures an IDS signature matching profile.
ids unauthorized-device-profile	Configures an IDS unauthorized device profile.
show ids profile	Displays all IDS profiles or a specific IDS profile.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids rap-wml-server-profile

```
ids rap-wml-server-profile <server-name>
  ageout <ageout>
  cache{disable|enable}
  clone <source>
  db-name <db-name>
  ip-addr <ip-addr>
  password <password>
  rap-wml-table <profile-name>
  type {mssql|mysql}
  user <user>
no ...
```

Description

This command to configure an IDS remote AP WML (MSSQL or MySQL) server profile.

Parameter	Description
<server-name>	Name of the remote AP WML server.
ageout <ageout>	Specifies the cache ageout period, in seconds. 0
cache	Enables or disables the cache.
clone <source>	Copies configuration settings from an existing profile.
db-name <db-name>	Specifies the name of the database.
ip-addr <ip-addr>	Specifies the IP address of the named WML server. 0.0.0.0
no	Negates any configured parameter.
password <password>	Specifies the password required for database login.
rap-wml-table <profile-name>	Specifies the name of the RAP WML Table profile.
type	Specifies the server type: <ul style="list-style-type: none">▪ MSSQL server▪ MySQL server
user <user>	Specifies the user name required for database login.

Example

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) # ids rap-wml-server-profile
mssqlserver type mssql ip-addr 10.4.11.11 db-name automatedtestdatabase
user sa password sa
ids rap-wml-table-profile mssqlserver table-name mactest_
undelimited timestamp-column time lookup-time 600
ids rap-wml-table-profile mssqlserver table-name mactest_delimited mac-
delimiter : timestamp-column time lookup-time 600
```

Related Commands

Command	Description
show rap-wml	Displays configuration information for the MSSQL or MySQL server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids rap-wml-table-profile

```
ids rap-wml-table-profile <table-name>
  clone <source>
  column-name <column-name>
  lookup-time <lookup-time>
  mac-delimiter <mac-delimiter>
  no
  table-name <table-name>
  timestamp-column <timestamp-column-name>
```

Description

This command configures an IDS remote AP WML table profile.

Parameter	Description
<table-name>	Name of an IDS remote AP WML table profile.
clone <source>	Copies data from another IDS remote AP WML table profile.
column-name <column-name>	Specifies the database column name containing the MAC address.
lookup-time <lookup-time>	Specifies how far back, in seconds, to look for the MAC address. Use 0 seconds to look up everything.
mac-delimiter <mac-delimiter>	Specifies the optional delimiter character for the MAC address in the database.
no	Negates the rap-wml table for the named server.
table-name <table-name>	Specifies the database table name.
timestamp-column <timestamp-column-name>	Specifies the database column name with the timestamp last seen.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) #ids rap-wml-server-profile mysqlserver type mysql
ip-addr 10.4.11.10 db-name automatedtestdatabase user sa password sa
```

```
ids rap-wml-table-profile mysqlserver table-name mactest_
undelimited timestamp-column time lookup-time 600
ids rap-wml-table-profile table-name mysqlserver mactest_delimited mac-
delimiter : timestamp-column time lookup-time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) # ids rap-wml-server-profile
mysqlserver type mssql ip-addr 10.4.11.11 db-name automatedtestdatabase
user sa password sa
ids rap-wml-table-profile mssqlserver table-name mactest_
undelimited timestamp-column time lookup-time 600
ids rap-wml-table-profile mssqlserver table-name mactest_delimited mac-
delimiter : timestamp-column time lookup-time 600
```

Related Commands

Command	Description
ids rap-wml-server-profile	Configure an IDS remote AP WML (MSSQL or MySQL) server profile and then use the <code>ids rap-wml-table-profile</code> command to configure the associated database table for the server.
show rap-wml	Displays configuration information for the MSSQL or MySQL server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RF Protect license.	Config mode on Mobility Conductor.

ids rate-thresholds-profile

```
ids rate-thresholds-profile <profile-name>
  channel-inc-time <channel-inc-time>
  channel-quiet-time <channel-quiet-time>
  channel-threshold <channel-threshold>
  clone <profile>
  no ...
  node-quiet-time <node-quiet-time>
  node-threshold <node-threshold>
  node-time-interval <node-time-interval>
```

Description

This command configures an IDS rate thresholds profile.

A profile of this type is attached to each of the following 802.11 frame types in the IDS denial of service profile:

- association frames
- disassociation frames
- deauthentication frames
- probe Request frames
- probe Response frames
- authentication frames

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. The name must be 1-63 characters.
channel-inc-time <channel-inc-time>	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm. 0 - 360000 seconds 15 seconds
channel-quiet-time <channel-quiet-time>	After a channel rate anomaly alarm has been triggered, the time that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file. 60-360000 seconds 900 seconds
channel-threshold	Number of specific frame types that must be exceeded within a specific interval in a channel to trigger an alarm. 0-100000 frames 300

Parameter	Description
<code>clone <source></code>	Copies an existing IDS rate thresholds profile.
<code>no</code>	Negates any configured parameter.
<code>node-quiet-time</code> <code><node-quiet-time></code>	After a node rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file. 60-360000 seconds 900 seconds
<code>node-threshold</code> <code><node-threshold></code>	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm. 0 -100000 frames 200
<code>node-time-interval</code> <code><node-time-interval></code>	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm. 1-120 seconds 15 seconds

Example

The following command configures frame thresholds:

```
(host) [mynode] (config) #ids rate-thresholds-profile Lobby
(host) [mynode] (IDS Rate Thresholds Profile "Lobby") #channel-threshold 250
```

Related Commands

Command	Description
<code>show ids rate-thresholds-profile</code>	Displays the IDS rate thresholds profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids signature-matching-profile

```
ids signature-matching-profile <profile-name>
  clone <source>
  no
  signature <profile-name>
```

Description

This command configures an IDS signature matching profile. You can include one or more predefined signature profiles or a user-defined signature profile in a signature matching profile.

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. 1-63 characters
clone <source>	Name of an existing IDS signature matching profile from which parameter values are copied.
no	Negates any configured parameter.
signature <profile-name>	Name of a signature profile. See ids signature-profile on page 717 .

Example

The following command configures a signature matching profile:

```
(host) [mynode] (config) IDS signature matching LobbyEast
(host) [mynode] (IDS Signature Matching Profile "LobbyEast") #signature
Null-Probe-Response
```

Related Commands

Command	Description
show ids signature-matching-profile	Displays the IDS signature matching profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids signature-profile

```
ids signature-profile <profile-name>
  bssid <mac-addr> [valid-ap]
  clone <source>
  dst-mac <mac-addr> [valid-ap]
  frame-type {assoc|auth|beacon|control|data|deauth|disassoc|mgmt|probe-request
  {ssid <ssid>}{ssid-length <ssid-length>}|probe-response {ssid <ssid>}{ssid-length
  <ssid-length>}}
  no
  payload <pattern> [offset <offset>]
  seq-num <seq-num>
  src-mac <mac-addr> [valid-ap]
```

Description

This command configures signatures for wireless intrusion detection.

Parameter	Description
<profile-name>	Name that identifies an instance of the profile. The name must be 1-63 characters.
bssid <mac-addr>	BSSID field in the 802.11 frame header.
valid-ap	Matches a valid AP SSID.
clone <source>	Name of an existing IDS signature profile from which parameter values are copied.
dst-mac <mac-addr>	Destination MAC address in the 802.11 frame header.
valid-ap	Matches a valid AP SSID.
frame-type	Type of 802.11 frame. For each type of frame, further parameters can be specified to filter and detect only the required frames.
assoc	Association frame type
auth	Authentication frame type
beacon	Beacon frame type
control	All control frames
data	All data frames
deauth	Deauthentication frame type

Parameter	Description
disassoc	Disassociation frame type
mgmt	Management frame type
probe-request	Probe request frame type
probe-response	Probe response frame type
ssid <ssid>	For beacon, probe-request, and probe-response frame types, specify the SSID as either a string or hex pattern. 0-32 bytes
ssid-length <ssid-length>	For beacon, probe-request, and probe-response frame types, specify the length, in bytes, of the SSID. 0-32 bytes
no	Negates any configured parameter.
payload <pattern>	Pattern at a fixed offset in the payload of an 802.11 frame. Specify the pattern to be matched as a string or hex pattern. 0-32 bytes
offset <offset>	When a payload pattern is configured, specify the offset in the payload where the pattern is expected to be found in the frame.
seq-num <seq-num>	Sequence number of the frame.
src-mac <mac-addr>	Source MAC address in the 802.11 frame header.
valid-ap	Matches a valid AP SSID.

Example

The following command configures a signature profile:

```
(host) [mynode] (config) #ids signature-profile floor4
(host) [mynode] (IDS Signature Profile "floor4") #frame-type assoc
(host) [mynode] (IDS Signature Profile "floor4") #src-mac 00:00:00:00:00:00
```

Related Commands

Command	Description
show ids signature-profile	Displays the IDS signature profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids unauthorized-device-profile

```
ids unauthorized-device-profile <profile-name>
  adhoc-using-valid-ssid-quiet-time <adhoc-using-valid-ssid-quiet-time>
  allow-well-known-mac [hsrp|iana|local-mac|vmware|vmware1|vmware2|vmware3]
  cfg-valid-11a-channel <channel>
  cfg-valid-11g-channel <channel>
  classification
  clone <source>
  detect-adhoc-network
  detect-adhoc-using-valid-ssid
  detect-bad-wep
  detect-ht-greenfield
  detect-invalid-mac-oui
  detect-misconfigured-ap
  detect-sta-assoc-to-rogue
  detect-unencrypted-valid-client
  detect-valid-client-misassociation
  detect-valid-ssid-misuse
  detect-wifi-direct-p2p-groups
  detect-windows-bridge
  detect-wireless-bridge
  detect-wireless-hosted-network
  ignore-adhoc-awdl-networks
  mac-oui-quiet-time <mac-oui-quiet-time>
  no
  oui-classification
  overlay-classification
  privacy
  prop-wm-classification
  protect-adhoc-enhanced
  protect-adhoc-network
  protect-adhoc-using-valid-ssid
  protect-high-throughput
  protect-ht-40mhz
  protect-misconfigured-ap
  protect-ssid
  protect-valid-sta x
  protect-wifi-direct-p2p-groups
  protect-windows-bridge
  protect-wireless-hosted-network
  require-wpa
  rogue-containment
  suspect-rogue-conf-level <suspect-rogue-conf-level>
  suspect-rogue-containment
  unencrypted-valid-client-quiet-time
  valid-and-protected-ssid <valid-and-protected-ssid>
  valid-oui <valid-oui>
  valid-wired-mac <valid-wired-mac>
  vendor-specific-ie-exclusion <oui> <oui type>
  wifi-direct-network-quiet-time
  wireless-bridge-quiet-time <wireless-bridge-quiet-time>
  wireless-hosted-network-quiet-time <wireless-hosted-network-quiet-time>
```

Description

This command configures detection of unauthorized devices, as well as rogue AP detection and containment. Unauthorized device detection includes the ability to detect and disable rogue APs and other devices that can potentially disrupt network operations.

Parameter	Description
<code><profile-name></code>	Name that identifies an instance of the profile. 1-63 characters
<code>adhoc-using-valid-ssid-quiet-time</code>	Time to wait, in seconds, after detecting an ad hoc network using a valid SSID, after which the check can be resumed. 60-360000 seconds 900 seconds
<code>allow-well-known-mac</code>	Allows devices with known MAC addresses to classify rogues APs. Depending on your network, configure one or more of the following options for classifying rogue APs: <ul style="list-style-type: none">▪ hsrp: Routers configured for HSRP, a Cisco proprietary redundancy protocol, with the HSRP MAC OUI 00:00:0c.▪ iana: Routers using the IANA MAC OUI 00:00:5e.▪ local-mac: Devices with locally administered MAC addresses starting with 02.▪ vmware: Devices with any of the following VMWare OUIs: 00:0c:29, 00:05:69, or 00:50:56▪ vmware1: Devices with VMWare OUI 00:0c:29.▪ vmware2: Devices with VMWare OUI 00:05:69.▪ vmware3: Devices with VMWare OUI 00:50:56. If you modify an existing configuration, the new configuration overrides the original configuration. For example, if you configure <code>allow-well-known-mac hsrp</code> and then configure <code>allow-well-known-mac iana</code> , the original configuration is lost. To add more options to the original configuration, include all of the required options, for example: <code>allow-well-known-mac hsrp iana</code> .

Parameter	Description
	<p>Use caution when configuring this command. If the neighboring network uses similar routers, those APs might be classified as rogues. If containment is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.</p> <p>To clear the well known MACs in the system, use the following commands:</p> <ul style="list-style-type: none"> ▪ <code>clear wms wired-mac</code>: This clears all of the learned wired MAC information on Mobility Conductor. ▪ <code>reload</code>: This reboots Mobility Conductor.
<code>cfg-valid-11a-channel <channel></code>	<p>List of valid 802.11a channels that third-party APs are allowed to use.</p> <p>34-165</p>
<code>cfg-valid-11g-channel <channel></code>	<p>List of valid 802.11b/g channels that third-party APs are allowed to use.</p> <p>1-14</p>
<code>classification</code>	<p>Enables or disables rogue AP classification. A rogue AP is one that is unauthorized and plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered to be interfering — it has the potential to cause RF interference but it is not connected to the wired network and thus does not represent a direct threat.</p>
<code>clone <source></code>	<p>Name of an existing IDS rate thresholds profile from which parameter values are copied.</p>
<code>detect-adhoc-network</code>	<p>Enables or disables detection of ad hoc networks.</p>
<code>detect-adhoc-using-valid-ssid</code>	<p>Enables or disables detection of ad hoc networks using valid or protected SSIDs.</p>
<code>detect-bad-wep</code>	<p>Enables or disables detection of WEP initialization vectors that are known to be weak or repeating. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and search for implementations that are still used by many legacy devices.</p>
<code>detect-ht-greenfield</code>	<p>Enables or disables detection of high-throughput devices advertising greenfield preamble capability.</p>

Parameter	Description
<code>detect-invalid-mac-oui</code>	Enables or disables checking of the first three bytes of a MAC address, known as the organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI checking causes an alarm to be triggered if an unrecognized MAC address is in use.
<code>detect-misconfigured-ap</code>	Enables or disables detection of misconfigured APs. An AP is classified as misconfigured if it is classified as valid and does not meet any of the following configurable parameters: <ul style="list-style-type: none"> ▪ valid channels ▪ encryption type ▪ list of valid AP MAC OUIs ▪ valid SSID list
<code>detect-sta-assoc-to-rogue</code>	Enables or disables detection of station association to rogue AP.
<code>detect-unencrypted-valid-client</code>	Enables or disables detection of unencrypted valid clients.
<code>detect-valid-client-misassociation</code>	Enables or disables detection of misassociation between a valid client and an unsafe AP. This setting can detect the following misassociation types: <ul style="list-style-type: none"> ▪ MisassociationToRogueAP ▪ MisassociationToExternalAP ▪ MisassociationToHoneypotAP ▪ MisassociationToAdhocAP ▪ MisassociationToHostedAP
<code>detect-valid-ssid-misuse</code>	Enables or disables detection of Interfering or Neighbor APs using valid or protected SSIDs.
<code>detect-wifi-direct-p2p-groups</code>	Enables or disables detection of WIFI-Direct P2P groups.
<code>detect-windows-bridge</code>	Enables or disables detection of Windows station bridging.
<code>detect-wireless-bridge</code>	Enables or disables detection of wireless bridging.
<code>detect-wireless-hosted-network</code>	If enabled, this feature can detect the presence of a wireless hosted network. When a wireless hosted network is detected this feature sends a "Wireless Hosted Network" warning level security log message and the <i>wlsxWirelessHostedNetworkDetected</i> SNMP trap.

Parameter	Description
	If there are clients associated to the hosted network, this feature will send a "Client Associated To Hosted Network" warning level security log message and the <i>wlsxClientAssociatedToHostedNetworkDetected</i> SNMP trap.
ignore-adhoc-awdl-networks	Ignore or process frames from adhoc AWDL networks.
mac-oui-quiet-time	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered. 60-360000 seconds 900 seconds
no	Negates any configured parameter.
oui-classification	Enables or disables OUI based rogue AP classification.
overlay-classification	Enables or disables overlay rogue AP classification.
privacy	Enables or disables encryption as a valid AP configuration.
prop-wm-classification	Enables or disables rogue AP classification through propagated wired MACs.
protect-adhoc-enhanced	Enable or disable advanced protection from open or WEP ad hoc networks. When enhanced ad hoc containment is carried out, a new repeatable event, syslog and SNMP trap will be generated for each containment event.
protect-adhoc-network	Enable or disable protection from ad hoc networks using WPA or WPA2 security. When ad hoc networks are detected, they are disabled using a DoS attack.
protect-adhoc-using-valid-ssid	Enable or disable protection from ad hoc networks using valid or protected SSIDs.
protect-high-throughput	Enable or disable protection of high-throughput (802.11n) devices.
protect-ht-40mhz	Enable or disable protection of high-throughput (802.11n) devices operating in 40 MHz mode.
protect-misconfigured-ap	Enable or disable protection of misconfigured APs.

Parameter	Description
protect-ssid	Enable or disable use of SSID by valid APs only.
protect-valid-sta	When enabled, does not allow valid stations to connect to a non-valid AP.
protect-wifi-direct-p2pgroups	Enable or disable protection from WIFI-Direct P2P Groups.
protect-windows-bridge	Enable or disable protection of a windows station bridging
protect-wireless-hosted-network	<p>When you enable the wireless hosted network protection feature, Mobility Conductor enforces containment on a wireless hosted network by launching a denial of service attack to disrupt associations between a Windows 7 software-enabled Access Point (softAP) and a client, and disrupt associations between the client that is hosting the softAP and any access point to which the host connects.</p> <p>When a wireless hosted network triggers this feature, wireless hosted network protection sends the Wireless Hosted Network Containment and Host of Wireless Network Containment warning level security log messages, and the <i>wlsxWirelessHostedNetworkContainment</i> and <i>wlsxHostOfWirelessNetworkContainment</i> SNMP traps.</p> <p>NOTE: The existing generic containment SNMP traps and log messages will also be sent when Wireless Hosted Network Containment or Host of Wireless Network Containment is enforced.</p>
require-wpa	When enabled, any valid AP that is not using WPA encryption is flagged as misconfigured.
rogue-containment	Rogue APs can be detected (see classification) but are not automatically disabled. This option automatically shuts down rogue APs. When this option is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.
suspect-rogue-conf-level <suspect-rogue-conf-level>	<p>Confidence level of suspected Rogue AP to trigger containment.</p> <p>When an AP is classified as a suspected rogue AP, it is assigned a 50% confidence level. If multiple APs trigger the same events that classify the AP as a suspected rogue, the confidence level increases by 5% up to 95%.</p>

Parameter	Description
	<p>In combination with suspected rogue containment, this option configures the threshold by which containment should occur. Suspected rogue containment occurs only when the configured confidence level is met.</p> <p>50-100%</p> <p>60%</p>
suspect-rogue-containment	<p>Suspected rogue APs are treated as interfering APs, thereby Mobility Conductor attempts to reclassify them as rogue APs. Suspected rogue APs are not automatically contained. In combination with the configured confidence level (see suspect-rogue-conf-level), this option contains the suspected rogue APs.</p>
unencrypted-valid-client-quiet-time <unencrypted-valid-client-quiet-time>	<p>Time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.</p> <p>60-360000 seconds</p> <p>900 seconds</p>
valid-and-protected-ssid <ssid>	List of valid and protected SSIDs.
valid-oui <valid-oui>	List of valid MAC OUIs.
valid-wired-mac <valid-wired-mac>	List of MAC addresses of wired devices in the network, typically gateways or servers.
vendor-specific-ie-exclusion <oui> <oui type>	<p>Configures exclusions for IDS containment based on vendor specific IE information. This feature allows APs to be exempted from containment even when the devices use randomized MAC addresses. ArubaOS allows for a maximum of five vendor OUI and OUI types to be defined for confinement exclusion.</p>
wifi-direct-network-quiet-time	<p>Time to wait in seconds after detecting a WIFI-Direct network, after which the check can be resumed. Minimum is 60 seconds</p>
wireless-bridge-quiet-time <wireless-bridge-quiet-time>	<p>Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.</p> <p>60-360000 seconds</p> <p>900 seconds</p>

Parameter	Description
wireless-hosted-network-quiet-time <wireless-hosted-network-quiet-time>	The wireless hosted network detection feature sends a log message and trap when a wireless hosted network is detected. The quiet time defined by this parameter sets the amount of time, in seconds, that must elapse after a wireless hosted network log message or trap has been triggered before an identical log message or trap can be sent again. 60-360000 seconds 900 seconds

Example

The following command copies the settings from the `ids-unauthorized-device-disabled` profile and then enables detection and protection from ad hoc networks:

```
(host) [mynode] (config) #ids unauthorized-device-profile floor7
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #unauth1
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #clone ids-
unauthorized-device-disable
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #detect-adhoc-
network
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #protect-adhoc-
network
```

Related Commands

Command	Description
show ids unauthorized-device-profile	Displays an IDS unauthorized device profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	The vendor-specific-ie-exclusion parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

ids wms-general-profile

```
ids wms-general-profile
  adhoc-ap-ageout-interval <adhoc-ap-ageout-interval>
  ap-ageout-interval <ap-ageout-interval>
  collect-stats
  detect-phony-bssid
  learn-ap
  learn-system-wired-macs
  no
  persistent-neighbor
  persistent-valid-sta
  phony-bssid-quiet-time <phony-bssid-quiet-time>
  poll-interval <poll-interval>
  poll-retries <poll-retries>
  propagate-wired-macs
  sta-ageout-interval <sta-ageout-interval>
  stat-update
```

Description

This command configures the IDS WLAN management system (WMS) general profile. The WLAN management system (WMS) on Mobility Conductor monitors wireless traffic to detect any new AP or wireless client station in the RF environment. When an AP or wireless client is detected, it is classified, and its classification is used to determine the security policies that should be enforced on the AP or client.

By default, non-Aruba APs that are connected on the same wired networks as Aruba APs are classified as “rogue” APs. Enabling AP learning classifies non-Aruba APs as “valid” APs. Typically, you would want to enable AP learning in environments with large numbers of existing non-Aruba APs and leave AP learning enabled until all APs in the network have been detected and classified as valid. Then, disable AP learning and reclassify any unknown APs as interfering.

VLAN Trunking

In deployments where Aruba APs are not placed on every VLAN and where it is *not* possible to trunk all VLANs to an Aruba AP, enable the parameter **learned-system-wired-mac**. When this is enabled, ArubaOS is able to classify rogues on all the VLANs that belong to a Mobility Conductor, as long as Aruba APs can see the rogues in the air. If there are VLANs in the network residing on a third party controller and if those VLANs are trunked to a port on a Mobility Conductor, enabling this feature will allow detection of rogues on those VLANs as well.

Mobility Conductor/Managed Device

When **learned-system-wired-mac** is enabled in a Mobility Conductor deployment, the learning of Wired and Gateway MACs will happen at each managed device. For topologies with managed devices in different geographical locations, the managed device collects the Wired and Gateway MAC info and passes it to the APs that are connected to it. Even though the locals do the collection of Wired and Gateway MACs, Mobility Conductor is still responsible for classification.

Parameter	Description
adhoc-ap-ageout-interval <adhoc-ap-ageout-interval>	Time, in minutes, that an ad hoc (IBSS) AP remains unseen before it is deleted (ageout) from the database. 0-10000 30 minutes
ap-ageout-interval <ap-ageout-interval>	Time, in minutes, that an AP remains unseen by any probes before it is deleted from the database. 0-10000 30 minutes
collect-stats	Enables or disables collection of statistics (up to 25,000 entries) on Mobility Conductor for monitored APs and clients.
detect-phony-bssid	Enable or disable phony BSSID detection.
learn-ap	Enables or disables "learning" of non-Aruba APs.
learn-system-wired-macs	Enables or disables "learning" of wired MACs.
no	Negates any configured parameter.
persistent-neighbor	Does not age out known AP neighbors.
persistent-valid-sta	Does not age out valid stations.
phony-bssid-quiet-time <phony-bssid-quiet-time>	Specify phony BSSID quiet time in minutes.
poll-interval <poll-interval>	Interval, in milliseconds, for communication between Mobility Conductor and Aruba AMs. Mobility Conductor contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics. 60000 milliseconds (1 minute)
poll-retries <poll-retries>	Maximum number of failed polling attempts before the polled AM is considered to be down. 2
propagate-wired-macs	Enable/disable propagation of the gateway wired MAC information.
sta-ageout-interval <sta-ageout-interval>	Time, in minutes, that a client remains unseen by any probes before it is deleted from the database. 30 minutes
stat-update	Enable/disable statistics updating in the database.

Example

The following command enables AP learning:

```
(host) [mynode] (IDS WMS General Profile) #learn-ap
```

The following command disables AP learning:

```
(host) [mynode] (IDS WMS General Profile) #no learn-ap
```

Related Commands

Command	Description
show ids wms-general-profile	Displays general statistics for the WMS configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ids wms-local-system-profile

```
ids wms-local-system-profile
  max-ap-threshold <max-ap-threshold>
  max-rbtree-entries <max-rbtree-entries>
  max-sta-threshold <max-sta-threshold>
  max-system-wm <max-system-wm>
  no
  override-svc-termination <override-svc-termination>
  periodic-ap-snapshot-interval <periodic-ap-snapshot-interval>
  periodic-rogue-ap-snapshot-interval <periodic-rogue-ap-snapshot-interval>
  periodic-sta-snapshot-interval <periodic-sta-snapshot-interval>
  system-wm-update-interval <system-wm-update-interval>
```

Description

This command configures the WLAN management system (WMS) service to terminate on individual managed devices instead of Mobility Conductor.

The WLAN management system (WMS) on the controller monitors wireless traffic to detect any new AP or wireless client station in the RF environment. When an AP or wireless client is detected, it is classified, and its classification is used to determine the security policies that should be enforced on the AP or client. By default, the WMS service is terminated at Mobility Conductor, which requires every AP across the network to communicate with the WMS service on Mobility Conductor. The IDS WMS local system profile includes a WMS service termination override parameter that optimizes limited bandwidth between the managed device and Mobility Conductor by allowing the AP communicate directly with the managed device to which it is associated.

When local WMS service termination is enabled, the WMS service on the managed device will:

- Perform device classification for associated APs
- Correlate events from associated APs
- Update the local WMS database
- Aggregate and redistribute WMS data such as wired MAC addresses, tarpit BSSIDs and valid or registered OUIs to associated APs

The devices and events detected by the managed device can (optionally) be sent to Mobility Conductor, allowing Mobility Conductor to update its database with AP, client and event information from that managed device. Note, however, that enabling this option increases the bandwidth usage between the managed device and Mobility Conductor.

The configuration parameters in IDS WMS local system profile enables local termination of the WMS service, sets maximum thresholds for the maximum number of managed APs and stations, and defines the intervals at which valid AP, rogue AP and station data is sent to the managed device. Increasing the max AP or max station threshold limits in the IDS local system profile will cause an increase in usage in the memory by WMS. In general, each entry will consume about 500 bytes of memory. If a setting is bumped up by 2000, then it will cause an increase in WMS memory usage by 1 MB.

Parameter	Description
max-ap-threshold	Sets the max threshold for the total number of APs. 0 to 50,000,000
max-rbtree-entries	Sets the max threshold for the total number of AP and station RBTREE entries.
max-sta-threshold	Sets the max threshold for the total number of stations.
max-system-wm	Sets the max number of system wired MAC table entries learned by the managed device. 1-2000 1000
no	Negates or deletes an existing parameter
override-svc-termination	Overrides the system-determined termination mode, and terminates WMS service at the managed device to which the AP is associated. Do not use this option if you have multiple managed devices in one location, as WMS will not operate correctly.
periodic-ap-snapshot-interval	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored APs. The (AMON) messages comprising the snapshot are spread over this interval. 60-360 minutes 180 minutes
periodic-rogue-ap-snapshot-interval	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored rogue APs. The (AMON) messages comprising the snapshot are spread over this interval. 5-360 minutes 30 minutes
periodic-sta-snapshot-interval	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored clients. The (AMON) messages comprising the snapshot are spread over this interval. 60-360 minutes 180 minutes
system-wm-update-interval	Sets the interval, in minutes, for repopulating the system wired MAC table at the managed device. 1-30 minutes 8 minutes

Example

The following commands first set the interval time for repopulating the MAC table to 10 minutes and then sets the maximum number of APs to 100:

```
(host) [mynode] (config) #ids wms-local-system-profile system-wm-update-  
interval 10  
(host) [mynode] (config)# ids wms-local-system-profile max-ap-threshold 100
```

Related Commands

Command	Modification
mgmt-server	Configures the management server profile.
ids management-profile	Manages the events correlation for IDS event traps and syslogs (logs).
show ids wms-local-system-profile	Displays the local WLAN management system (WMS) service profile settings .

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ifmap

```
ifmap cppm
  enable
  no
  server host <host>
    port <port>
      username<username>
      passwd <password>
```

Description

This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.

Parameter	Description
enable	Enables the IFMAP protocol.
server	Configures the ClearPass Policy Manager IF-MAP server.
host <host>	IP address or hostname of the ClearPass Policy Manager IF-MAP server.
port <port>	Port number for the ClearPass Policy Manager IF-MAP server. 1-65535 443
username <username>	Username for the user who performs actions on the ClearPass Policy Manager IF-MAP server. The name must be between 1-255 bytes in length.
passwd <password>	Password of the user who performs actions on the ClearPass Policy Manager IF-MAP server. The password must be between 6-100 bytes in length.

Example

This example configures IFMAP and enables it.

```
(host) [md] (config) #ifmap
(host) [md] (config) #ifmap cppm
(host) [md] (CPPM IF-MAP Profile) #server host <host>
(host) [md] (CPPM IF-MAP Profile) #port <port>
(host) [md] (CPPM IF-MAP Profile) #passwd <psswd>
(host) [md] (CPPM IF-MAP Profile) #enable
```

Related Commands

Command	Description
show ifmap	This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on managed device.

interface cellular

```
interface cellular ip access-group session <name>
interface cellular ip nat outside
interface cellular bandwidth-contract {app | appcategory} <appname>
    <STRING> [upstream | downstream]
interface cellular bandwidth-contract exclude [app | appcategory]
    <appname>
interface cellular bandwidth-contract <STRING> [upstream | downstream]
interface cellular transmit max-rate {kbits | mbits}
```

Description

This command allows you to specify an ingress or egress ACL to the cellular interface of an EVDO modem.

Parameter	Description
<code>interface cellular</code>	Configures the cellular interface.
<code>ip access-group session <name></code>	Enter the name or number of the access group you want to apply to the EVDO modem.
<code>ip nat outside</code>	Source NAT all traffic routed from this cellular interface.
<code>bandwidth-contract {app appcategory exclude <STRING>}</code>	Configures the egress bandwidth contract for the physical interface.
<code><appname></code>	Specifies the app name or the app category name.
<code>upstream</code>	Apply the bandwidth-contract to upstream.
<code>downstream</code>	Apply the bandwidth-contract to downstream.
<code>transmit max-rate {kbits mbits}</code>	Specify transmit rate-limit configuration in kbits or mbits.

Example

```
(host) [mynode](config-submode)#ip access-group session 3
(host) [mynode](config-submode)#bandwidth-contract app myapp bc1
downstream
```

Related Command

Command	Description
show interface cellular access-group	List the Access groups configured on the cellular interface.

Command History

Release	Modification
ArubaOS 8.2.0.0	Updated the new syntax as ip access-group session <name> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration Mode (config-submode) of Mobility Conductor.

interface gigabitethernet

```
interface gigabitethernet <slot>/<module>/<port>
  bandwidth-contract <name>|{{app <app-name>|appcategory <app-category-name>} <bw-
  contract-name>} upstream|downstream [exclude]

  dac-alternate-linkup
  description <string>
  duplex {auto|full|half}
  ip access-group {in|out|session {vlan <vlanId>}} <name>
  jumbo
  lacp {group|port-priority|timeout}
  lldp {fast-transmit-counter <1-8>|fast-transmit-interval <1-3600>|med|proprietary
  [<neighbor><discovery>]|receive|sys-tlv<disable>|transmit|transmit-hold <1-
  100>|transmit-interval <1-3600> }600}
  no ...
  openflow-disable
  poe
  port monitor {gigabitethernet <slot>/<module>/<port> | port-channel <pid>}
  priority-map <name>
  sfp-alternate-detection
  shutdown
  spanning-tree {[bpduguard]|[cost <value>]|[point-to-point]|[port-priority
  <value>]|[portfast] [vlan]}
  speed {10|100|auto}
  speed-mode {10Gbps|1Gbps|40Gbps}
  switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan
  [<vlans>|add <vlans>|all|except <vlans>|remove <vlans>|<WORD>]| native vlan
  <vlan>}|port-security maximum <num>}
  transmit
  trusted {vlan <word>}
  tunneled-node-port
  xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan <vlan>}
```

Description

This command configures a GigabitEthernet interface. Use this command to configure settings for Mobility Conductor interface, including duplex, LLDP and switchport settings. You can issue the **show port status** command to obtain information about the interfaces currently available on the Mobility Conductor.

Interface Bandwidth Contracts

7000 Series controllers have the ability to classify and identify applications on the network. You can create bandwidth contracts to limit traffic for individual applications (or categories of applications) either sent from or received by a selected interface. There are two basic models for using this feature.

■ **Limiting lower-priority traffic:** If there is a lower-priority application or application type that you want to limit, apply a bandwidth contract just to that application, and allow all other application traffic to pass without any limits.

Protecting higher-priority traffic: If you want to guarantee bandwidth for a company-critical application or application group, you can add that application to an exception list, then apply a bandwidth contract to all remaining traffic.

You can apply bandwidth contracts using one or both of these models. Each interface supports up to 64 bandwidth contracts.

Interface contract Precedence

An interface bandwidth contract is applied to downstream traffic before a user-role bandwidth contract is applied, and for upstream traffic, the user-role bandwidth contract is applied before the interface bandwidth contract. For all traffic using compression and encryption, bandwidth contracts are applied after that traffic is compressed and encrypted. If you apply more than one bandwidth contract to any specific category type, then the bandwidth contracts are applied in the following order:

A contract that explicitly excludes an application

A contract that explicitly excludes an application category

A contract that applies to a specific application

A contract that applies to a specific application category

A generic bandwidth contract, not specific to any application or application category

Parameter	Description
<code><slot/module/port></code>	Interface in <code><slot>/<module>/<port></code> format.
<code>bandwidth-contract</code>	Apply a bandwidth contract to all upstream of downstream traffic, or to traffic for a specified application or application category
<code><name></code>	Name of a bandwidth contract configured with the aaa bandwidth-contract command. If you specify a bandwidth contract name <i>before</i> you specify an application or application category, the bandwidth contract is applied to all downstream or upstream traffic.
<code>app <name></code>	Name of the application to which the bandwidth contract is applied. For a complete list of supported applications, issue the command <code>show dpi application all</code> .
<code>appcategory <name></code>	Name of the application category to which the bandwidth contract is applied. For a complete list of supported applications, issue the command <code>show dpi application category all</code> .

Parameter	Description
<code>downstream</code>	Apply the bandwidth contract to downstream traffic.
<code>upstream</code>	Apply the bandwidth contract to upstream traffic.
<code>exclude</code> <code><app> <appcategory></code>	Use this parameter to exclude application or application category traffic from a bandwidth contract.
<code>dac-alternate-linkup</code>	Enables alternate configuration to bring up link of DAC. Required for some DAC cables.
<code>description</code>	String that describes this interface.
<code>duplex</code>	Transmission mode on the interface: full or half-duplex or auto to automatically adjust transmission. <code>auto/full/half</code> <code>auto</code>
<code>ip access-group</code>	Applies the specified ACL to the interface. Use the <code>ip access-list</code> command to configure an ACL. This parameter requires the PEFNG license.
<code>in</code>	Applies ACL to interface's inbound traffic.
<code>out</code>	Applies ACL to interface's outbound traffic.
<code>session</code>	Applies session ACL to interface and optionally to a selected VLAN associated with this port.
<code>jumbo</code>	Enables or disables jumbo frame MTU configured via firewall on a port. <code>disabled</code>
<code>lACP</code>	Configure an LACP group to the interface.
<code>group <id> mode</code> <code>[active passive]</code>	Enter the LAG number (0-7) and specify the mode (active or passive). <ul style="list-style-type: none"> ■ Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets. ■ Passive mode—the interface is not in

Parameter	Description
	<p>an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.</p>
port-priority	<p>Enter the port-priority value. The higher the value, the lower the priority.</p> <p>1-65535 255</p>
timeout	<p>Enter the keyword long to set the LACP session to 90 seconds. Enter the keyword short to set the LACP session to 3 seconds.</p> <p>90</p>
lldp	<p>Configures an LLDP functionality on an interface.</p>
fast-transmit-counter	<p>Set the number of the LLDP data units sent each time fast LLDP data unit transmission is triggered.</p> <p>1-8 4</p>
fast-transmit-interval	<p>Set the LLDP fast transmission interval in seconds.</p> <p>1-3600 1</p>
med	<p>Enables the LLDP MED protocol.</p> <p>disabled</p>
proprietary neighbor discovery	<p>Configures proprietary neighbor discovery.</p>
receive	<p>Enables processing of LLDP PDU received.</p> <p>disabled</p>
sys-tlv disable	<p>Disables system TLV options.</p> <p>enabled</p>
transmit	<p>Enables LLDP PDU transmit.</p> <p>disabled</p>

Parameter	Description
transmit-hold <1-100>	Set the transmit hold multiplier. 1-100 4
transmit-interval <1-3600>	Sets the transmit interval in seconds. 1-3600 30
no	Negates any configured parameter.
openflow-disable	Enables or disables Openflow on Gigabit Ethernet. disabled
poe	Enables PoE on the interface. enabled
cisco	Enables Cisco-style PoE on the interface. disabled
port monitor gigabitethernet port-channel	Monitors another interface on the managed device.
priority-map	Applies a priority map to the interface. Use the <code>priority-map</code> command to configure a priority map which allows you to map ToS and CoS values into high priority traffic queues.
sfp-alternate-detection	Enables detection of SFP+ via alternative communications protocol. This parameter is required for some SFP+ transceivers.
shutdown	Causes a hard shutdown of the interface.
spanning-tree	Enables Rapid spanning tree or Per-VLAN spanning tree. enabled
bpduguard	Enables bpduguard on the edge ports. disabled
cost	Administrative cost associated with the spanning tree. The cost prioritizes routing to the destination. The lower the cost, the higher the priority. 1-65535

Parameter	Description
	4
point-to-point	Set interface as point to point. disabled
port-priority	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge. 1-255 1.28
portfast	Enables forwarding of traffic from the interface. disabled
vlan	Configure a VLAN instance or a range of VLAN IDs for spanning tree. 1-4094 disabled
speed	Sets the interface speed: 10 Mbps, 100 Mbps, 1000 Mbps, or auto configuration. 10 100 1000 auto auto
speed-mode {10Gbps 1Gbps 40Gbps }	Sets the interface speed-mode to one of the following values: <ul style="list-style-type: none"> ▪ 10 Gbps- - You can configure this on the ports, G0/0/0, G0/0/4, G0/0/8, and G0/0/12. ▪ 1 Gbps- - You can configure this on the ports, G0/0/8 and G0/0/12. ▪ 40 Gbps- - You can configure this on the ports, G0/0/0 and G0/0/4. The port range details are as follows: <ul style="list-style-type: none"> ▪ G0/0/0 - When applied on this port, the speed change is applicable to the port range 0/0/0 - 0/0/3. ▪ G0/0/4 - When applied on this port, the speed change is applicable to the port range 0/0/4 - 0/0/7. ▪ G0/0/8 - When applied on this port, the

Parameter	Description
	<p>speed change is applicable to the port range 0/0/8 - 0/0/11.</p> <ul style="list-style-type: none"> ■ G0/0/12 - When applied on this port, the speed change is applicable to the port range 0/0/12 - 0/0/15. <p>10 1 40</p> <p>NOTE: This parameter is applicable only to Aruba 7280 controllers.</p> <p>NOTE: You must reboot the controller after configuring this parameter.</p>
switchport	Sets switching mode parameters for the interface.
access vlan <id>	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.
mode {access trunk}	<p>Sets the mode of the interface to access or trunk mode only.</p> <p>access trunk</p> <p>access</p>
<pre>port-security maximum <num> [level [[drop] [logging] [shutdown interval <seconds>]]</pre>	<p>Sets the port security parameters such as the maximum number of addresses that can be configured on the port. Upon exceeding the maximum limit, the port drops the packets on the port.</p> <p>You can also set one of the following levels for dropping the packets on exceeding the limit:</p> <ul style="list-style-type: none"> ■ drop—drops the packets ■ logging—drops the packets and records a message in the log file. This is the default level. ■ shutdown—drops the packet, records a log message, and shuts the port down for the specified time interval.

Parameter	Description
<pre>trunk {allowed vlan {<vlans> add <vlans> all except <vlans> remove <vlans> <WORD>} native vlan <vlan>}}</pre>	<p>Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. You can also remove all the VLANs from the list of allowed VLANs configured on a trunk port. Specify native to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.</p>
<pre>transmit max-rate mbits <txrate> scheduler-profile <profile-name></pre>	<p>Sets a maximum transmit rate in Mbps and assigns a scheduler profile. Allowed range for maximum transmit rate is 1-100 Mbps.</p>
<pre>trusted</pre>	<p>Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to the managed device, set the port to be trusted.</p> <p>enabled</p>
<pre>vlan <word></pre>	<p>Sets the supplied range of VLANs as trusted. All remaining become untrusted automatically.</p> <p>For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the <code>no trusted vlan</code> command to explicitly make an individual VLAN untrusted. The <code>no trusted vlan</code> command is additive and adds given vlans to the existing untrusted vlan set.</p> <p>However, if you execute the <code>trusted vlan <word></code> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs.</p> <p>A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.</p> <p>1-4094</p>

Parameter	Description
tunneled-node-port	Enable tunneled node capability on the interface. disabled
xsec	Enables and configures the Extreme Security (xSec) protocol. NOTE: You must purchase and install the xSec software module license in the Mobility Conductor.
point-to-point	MAC address of the managed device that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the managed device to each other. The key must be the same on both managed device.
allowed vlan	VLANs that are allowed on the xSec tunnel.
mtu	(Optional) MTU size for the xSec tunnel.
vlan	xSec VLAN ID. For managed device-to-managed device communications, both managed device must belong to the same VLAN. 1-4094

Example

The following commands configure an interface as a trunk port for a set of VLANs:

```
(host) [mynode] (config) # interface gigabitethernet 0/0/0
(host) [mynode] (config-range)# switchport mode trunk
(host) [mynode] (config-range)# switchport trunk native vlan 10
(host) [mynode] (config-range)# switchport trunk allowed vlan 1,10,100
```

The following commands configure trunk port 0/0/0 with test-acl session for VLAN 2.

```
(host) [mynode] (config) # interface range gigabitethernet 0/0/0
(host) [mynode] (config-range)# switchport mode trunk
(host) [mynode] (config-range)# ip access-group
(host) [mynode] (config-range)# ip access-group test session vlan 2
```

The following commands configure a interface bandwidth contract for a high-priority application.

```
(host) [mynode] (config) # interface gigabitethernet 0/0/1
```

```
(host) [mynode] (config) # bw-contract protectskype4b exclude app alg-  
skype4b-voice downstream
```

Related Commands

Command	Description
<code>show interface gigabitethernet</code>	Displays information about a specified Gigabit Ethernet port.

Command History

Release	Modification
ArubaOS 8.3.0.0	A new parameter, <code>speed-mode</code> , was added.
ArubaOS 8.2.0.0	The following changes were introduced: <ul style="list-style-type: none">■ Updated the new syntax as ip access-group {in out session {vlan <vlanId>}} <name>■ A new sub parameter <WORD> was added under <code>switchport trunk allowed</code> parameter. You can specify none to remove all the VLANs from the list of allowed VLANs configured on the trunk port.■ A new parameter, <code>sfp-alternate-detection</code>, was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The <code>ip access-group</code> parameter requires the PEFNG license. The xsec parameter requires the xSec license.	Config mode on Mobility Conductor.

interface loopback

```
interface loopback
  ip address <ipaddr>
  ipv6 address <ipv6-prefix>
  no ...
```

Description

This command configures the loopback address on Mobility Conductor. If configured, the loopback address is used as Mobility Conductor's IP address. If you do not configure a loopback address for Mobility Conductor, the IP address assigned to VLAN 1 is used as Mobility Conductor's IP address. After you configure or modify a loopback address, you need to reboot Mobility Conductor.

Parameter	Description
ip address	Host IP address in dotted-decimal format. This address is routed from all external networks.
ipv6 address	Host IPv6 address that can be routed from all external networks.
no	Negates any configured parameter.

Example

The following command configures a loopback address:

```
(host) [mynode] (config) #interface loopback
(host) [mynode] (config-submode)#ip address 10.2.22.220
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system.	Config mode on Mobility Conductor.

interface mgmt

```
interface mgmt
  dhcp
  ip address <ipaddr> <ipmask> [vlan-tag <vlanid>]
  ipv6 address <ipaddr>/<prefix-length> [vlan-tag <vlanid>]
  no ...
  shutdown
```

Description

This command configures the out-of-band Ethernet management port on controller.

Syntax

Parameter	Description
dhcp	Enables DHCP on the interface. NOTE: This parameter is available only for AOS version 8.9 or earlier.
ip address	Configures an IP address and netmask on the interface.
vlan-tag <vlanid>	(Optional) Tags the management interface with the specified VLAN ID.
ipv6 address <ipaddr>	Configures an IPv6 address on the interface.
vlan-tag <vlanid>	(Optional) Tags the management interface with the specified VLAN ID.
no	Negates any configured parameter.
shutdown	Causes a hard shutdown of the interface.

Usage Guidelines

Execute this command on the device level from the Mobility Conductor. This command is applicable only for the 7000 Series platforms.

Use the **show interface mgmt** command to view the current status of the management port.

Example

The following command configures an IP address on the management interface:

```
(host) [mynode] (config) #interface mgmt
(host) [mynode] (config-submode) #ip address 10.1.1.1 255.255.255.0
```

Command History

Release	Modification
ArubaOS 8.0.1.0	vlan-tag optional sub-parameter was introduced under the ip address and ipv6 address parameters.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
7000 Series controllers	Base operating system.	Config mode on Mobility Conductor.

interface port-channel

```
interface port-channel <id>
  description <LINE>
  gigabitethernet <slot/module/port>
  ip access-group {in <name>|out <name>|session <name>|vlan <vlanId> {session
<name>}}
  jumbo
  no ...
  openflow-disable
  shutdown
  spanning-tree [bpduguard|cost <value>|point-to-point|port-priority
<value>|portfast [trunk]|vlan {range <WORD>|<vlanid>}}
  switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan
<vlans>|add <vlans>|all|except <vlans>|remove <vlans>| native vlan <vlan>}
  trusted {vlan [add|remove] <word>}
  xsec {{point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>}}|vlan <vlan>}
```

Description

This command configures an Ethernet port channel.

A port channel allows you to aggregate ports on a managed device. You can configure a maximum of 8 port channels per supported managed device with a maximum of 8 interfaces per port channel.

Note the following when setting up a port channel between a managed device and a Cisco switch (such as a Catalyst 6500 Series Switch):

- There must be no negotiation of the link parameters.
- The port-channel mode on the Cisco switch must be “on”.

Parameter	Description
<id>	ID number for this port channel. 0-7
description <LINE>	A character string describing this port-channel. up to 60 characters
gigabitethernet <slot/module/port>	Adds the specified GigabitEthernet interface to the port channel.
ip <access-group>	Applies the specified ACL to the interface. Use the <code>ip access-list</code> command to configure an ACL. This command requires the PEFNG license.

Parameter	Description
<code>in <name></code>	Applies ACL to interface's inbound traffic.
<code>out <name></code>	Applies ACL to interface's outbound traffic.
<code>session <name></code>	Applies session ACL to interface and optionally to a selected VLAN associated with this port.
<code>vlan <vlanId> {session <name>}</code>	Applies session ACL to VLAN. 1-4094
<code>jumbo</code>	Enables or disables jumbo frame MTU configured via firewall on a port channel. Disabled
<code>no</code>	Negates any configured parameter.
<code>openflow-disable</code>	Enables or disables Openflow on the port channel. Disabled NOTE: This parameter is available only for AOS version 8.9 or earlier.
<code>shutdown</code>	Causes a hard shutdown of the interface.
<code>spanning-tree</code>	Enables spanning tree.
<code>bpduguard</code>	Enables BPDU guard on the port channel. Disabled
<code>cost <value></code>	Specify the cost value of the spanning tree path for an interface. 1 - 65535
<code>point-to-point</code>	Configures the interface as a point to point link.
<code>port-priority <value></code>	Specify the spanning tree priority for the interface. 1 - 255
<code>portfast [trunk]</code>	Enables forwarding of traffic from the interface. Optionally you can choose a trunk port for forwarding the traffic.
<code>vlan {range <WORD> <vlanid>}}</code>	Configure a VLAN instance or a range of VLAN IDs for the

Parameter	Description
switchport	Sets switching mode parameters for the interface.
access vlan <vlanId>	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.
mode {access trunk}	Sets the mode of the interface to access or trunk mode only.
port-security maximum <num>	Sets the maximum number of MAC addresses that can be configured on the port channel. 16-32768
trunk {allowed vlan {<vlans> add <vlans> all except <vlans> remove <vlans>} native vlan <vlan>}}	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. Optionally you can specify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.
trusted	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to a managed device, set the port to be trusted. disabled
vlan [add remove] <word>	Sets the specified range of VLANs as trusted. All remaining become untrusted automatically. For example, if you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the <code>no trusted vlan</code> command to explicitly make an individual VLAN untrusted. The <code>no trusted vlan</code> command is additive and adds given vlans to the existing untrusted vlan set.

Parameter	Description
	<p>However, if you execute the <code>trusted vlan <word></code> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs.</p> <p>A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.</p> <p>1-4094</p>
<code>xsec</code>	<p>Enables and configures the Extreme Security (xSec) protocol.</p> <p>You must purchase and install the xSec software module license in the managed device.</p>
<code>point-to-point</code>	<p>MAC address of the device that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the device to each other. The key must be the same on both devices.</p>
<code>allowed vlan</code>	VLANs that are allowed on the xSec tunnel.
<code>mtu</code>	(Optional) MTU size for the xSec tunnel.
<code>vlan</code>	<p>xSec VLAN ID. For managed device-to-managed device communications, both managed devices must belong to the same VLAN.</p> <p>1-4094</p>

Example

The following command configures a port channel:

```
(host) (config) #interface port channel 7
(host) [mynode] (config-submode) #gigabitethernet 0/0/1
(host) [mynode] (config-submode) #gigabitethernet 0/0/2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Updated the new syntax as ip access-group {in <name> out <name> session <name> vlan <vlanId> {session <name>}} .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The <code>ipaccess-group</code> parameter requires the PEFNG license. The xsec parameter requires the xSec license.	Config mode on Mobility Conductor.

interface range

```
interface range gigabitethernet <slot>/<module-start>/<port-start>-<module-
end>/<port-end>
  ip access-group {in|out|session {vlan <vlanId>}} <acl>_name>
  lacp
  lldp
  no
  shutdown
  switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan
<vlans>|add <vlans>|all|except <vlans>|remove <vlans>}|
  native vlan <vlan>}}
  trusted {vlan <word>}
```

Description

This command configures a range of GigabitEthernet interfaces on the managed device.

Parameter	Description
range	Range of Ethernet ports in the format <slot>/<module>/<port>-<port>. where <slot>/<module>/<port> is the interface.
duplex	Transmission mode on the interface: full- or half-duplex or auto to automatically adjust transmission. auto/full/half auto
ip access-group	Applies the specified ACL to the interface. Use the ip access-list command to configure an ACL.
in	Applies ACL to interface's inbound traffic.
out	Applies ACL to interface's outbound traffic.
session	Applies session ACL to interface and optionally to a selected VLAN associated with this range of ports.
lacp	Configure an LACP group to the interface.
group <id> mode [active passive]	Enter the LAG number (0-7) and specify the mode (active or passive). 1. Active mode—the interface is in active negotiating state. LACP runs on any link

Parameter	Description
	<p>that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets.</p> <p>2. Passive mode—the interface is not in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.</p>
<code>port-priority <value></code>	<p>Enter the port-priority value. The higher the value, the lower the priority.</p> <p>1-65535 255</p>
<code>timeout</code>	<p>Enter the keyword long to set the LACP session to 90 seconds. Enter the keyword short to set the LACP session to 3 seconds.</p> <p>90</p>
<code>lldp</code>	<p>Configures an LLDP functionality on an interface.</p>
<code>fast-transmit-counter</code>	<p>Set the number of the LLDP data units sent each time fast LLDP data unit transmission is triggered.</p> <p>1-8 4</p>
<code>fast-transmit-interval</code>	<p>Set the LLDP fast transmission interval in seconds.</p> <p>1-3600 1</p>
<code>med</code>	<p>Enables the LLDP MED protocol.</p> <p>disabled</p>
<code>receive</code>	<p>Enables processing of LLDP PDU received.</p> <p>disabled</p>
<code>transmit</code>	<p>Enables LLDP PDU transmit.</p>

Parameter	Description
	disabled
transmit-hold <1-100>	Set the transmit hold multiplier. 1-100 4
transmit-interval <1-3600>	Sets the transmit interval in seconds. 1-3600 30
no	Negates any configured parameter.
shutdown	Causes a hard shutdown of the interface.
switchport	Sets switching mode parameters for the interface.
access vlan	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.
mode	Sets the mode of the interface to access or trunk mode only.
trunk {allowed vlan {<vlans> add <vlans> all except <vlans> remove <vlans>} native vlan <vlan>}}	Sets the interfaces as trunk ports for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. Optionally you can specify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.
trusted	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to the managed device, set the port to be trusted. enabled
vlan <word>	Sets the specified range of VLANs as trusted. All remaining become untrusted automatically.

Parameter	Description
	<p>For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the no trusted vlan command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set.</p> <p>However, if you execute the trusted vlan <word> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs.</p> <p>1-4094</p> <p>NOTE: A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.</p>

Example

The following command configures a range of interface as a trunk port for a set of VLANs:

```
(host) [00:0b:86:99:88:17] (config) #interface range gigabitethernet 0/0/0-0/17
(host) [00:0b:86:99:88:17] (config-submode)#switchport mode trunk
(host) [00:0b:86:99:88:17] (config-submode)#switchport trunk native vlan 10
(host) [00:0b:86:99:88:17] (config-submode)#switchport trunk allowed vlan 1,10,100
```

Related Commands

Command	Description
show port status	This command displays information about the interfaces available on the managed device. You can execute this command only on a hardware platform that acts as a managed device or as a stand-alone controller.

Command History

Release	Modification
ArubaOS 8.2.0.0	Updated the new syntax as ip access-group {in out session {vlan <vlanId>}} <acl_name> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

interface tunnel

```
interface tunnel <number>
  autogenerate peer <peer-mac-address>
  description <string>
  inter-tunnel-flooding
  ip
    access group in <acl-name>
    address {internal | pool tunnel-pool <pool-name> |{<ipaddr> <netmask>}}
    ospf
      area <area-id>
      authentication message-digest
      cost <value>
      dead-interval <value>
      hello-interval <value>
      message-digest-key <id> <pwd>
      priority <value>
      retransmit-interval <value>
      transmit-delay <value>
    ipv6 address X:X:X:X::X
  mtu <mtu>
  no ...
  openflow-enable
  shutdown
  trusted [vlan add <word>|remove <word>|<word>]
  tunnel
    destination <ip-addr>|{ipv6 <ipv6-addr>}
    keepalive icmp <ipaddr> <next-hop>
    keepalive cisco|{<interval> <retries>}
    mode gre {ip|ipv6|<num>}
    source
      controller-ip
      ipv6 {controller-ip|loopback|{vlan <vlanid>}|<ipv6-addr>}
      loopback
      vlan <vlanid>
      <ip-addr>
    vlan add <word>|remove <word>|<word>
```

Description

This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device. The default is an IPv4 Layer-3 GRE tunnel (**tunnel mode gre ip**).



In Layer-3 GRE tunnels, IPv6 encapsulated in IPv4 and IPv4 encapsulated in IPv6 are not supported. The only Layer-3 GRE modes supported are IPv4 encapsulated in IPv4 and IPv6 encapsulated in IPv6.

You can direct traffic into the tunnel using a static route (by specifying the tunnel as the next hop for a static route) or a session-based ACL.

Parameter	Description
<code><number></code>	<p>Tunnel Identification number.</p> <p>The tunnel ID used here does not have to match the tunnel ID used in the other managed device.</p> <p>1-16777215</p>
<code>autogenerate peer <peer-mac-address></code>	<p>Auto generates the tunnel endpoint for the specified peer device.</p>
<code>description</code>	<p>String that describes this tunnel.</p>
<code>inter-tunnel-flooding</code>	<p>Enables inter-tunnel flooding.</p> <p>Enabled</p>
<code>ip access group in <acl-name></code>	<p>Attach a route ACL to a L3 GRE tunnel interface.</p> <p>When you associate a routing ACL to inbound traffic on a managed device terminating a L3 GRE tunnel, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group. For more information on creating a routing ACL, see ip access-list route.</p>
<code>ip address</code> <code>{internal pool tunnel-pool <pool-name></code> <code> {<ipaddr> <netmask>}}</code>	<p>IP address of the Layer 3 tunnel. This represents the entrance to the tunnel.</p> <p>NOTE: This address</p>

Parameter	Description
	<p>should be a unique, non-routable IP address.</p> <p>Enter one of the following values:</p> <ul style="list-style-type: none"> ▪ internal: IP address is allocated from the Remote-Node pool. ▪ pool tunnel-pool <pool-name>: IP address is allocated from the specified tunnel pool. ▪ <ipaddr>: An IPv4 address. <p>NOTE: The IP address should not be part of any subnet in your network, nor does it have to be routable in your network. It is used as a gateway for routing your private subnets (i.e., non-routable VLANs) within the GRE tunnel.</p> <ul style="list-style-type: none"> ▪ <netmask>: IP subnet mask.
ipv6	<p>IPv6 address of the Layer-3 GRE tunnel.</p> <p>NOTE: This IP address can be configured only for a Layer-3 GRE tunnel (refer to the "<i>mode gre</i>" parameter below for details).</p>

Parameter	Description
mtu	MTU size for the interface. 1024 - 9216 Enabled, IPv4: 1100, IPv6: 1500
no	Negates any configured parameter.
openflow-enable	Enables OpenFlow on the tunnel. Disabled
shutdown	Causes a hard shutdown of the interface.
trusted [vlan {add <word>} {remove <word>} <word>]	<ul style="list-style-type: none"> ■ When Trusted is enabled: Any device can send any traffic through the GRE tunnel without having to be authenticated. Trusted VLANs are supported on a single Layer-2 GRE tunnel. ■ Use vlan add <word> to add VLANs to the current trusted list. Disabled <p>NOTE: <word> represents a VLAN range.</p> <ul style="list-style-type: none"> ■ Use vlan remove <word> to remove VLANs from the current trusted list. <p>NOTE: <word></p>

Parameter	Description
	<p>represents a VLAN range.</p> <ul style="list-style-type: none"> ■ When Trusted is disabled: <p data-bbox="1208 447 1398 1115">Any device that is a source of traffic and is sent through the tunnel must be authenticated to be able to send the traffic. If the device is not authenticated, traffic from that device will be subject to the restrictions of the Initial Role specified in the Wired Access AAA Profile. This is the default. Untrusted VLANs are supported on a single Layer-2 GRE tunnel.</p> <p data-bbox="1170 1119 1386 1228">For related information, see aaa authentication wired.</p>
tunnel	<p>Configures tunneling. The default is an IPv4 Layer-3 GRE tunnel.</p> <pre data-bbox="1170 1381 1317 1413">mode gre ip</pre>
destination <ip-addr> {ipv6 <ipv6-addr>}	<p>The destination IP address (IPv4 or IPv6) for the GRE tunnel endpoint.</p>
keepalive icmp	<p>Enables sending periodic ICMP (ping) keepalive frames on the tunnel to determine the status of the tunnel (up or down).</p>

Parameter	Description
	Disabled
<ipaddr>	IP address of the ping destination.
<next-hop>	<p>Router IP address belonging to any of the L2 GRE tunnel - vlans . This parameter is mandatory only for L2 GRE tunnel.</p> <p>Disabled</p>
<pre>keepalive cisco {<interval> <retries>}</pre>	<p>Enables sending of periodic keepalive frames on the tunnel to determine the tunnel status (up or down). You can optionally set the interval at which keepalive frames are sent, and the number of times the frames are resent before a tunnel is considered to be down.</p> <p>Disabled</p> <p>NOTE: Executing the <code>no tunnel keepalive</code> command disables the keepalive frames, but retains the configured interval and retry values.</p>

Parameter	Description
	<p>The <cisco> option enables keepalive interoperability for Layer-3 tunnels between managed devices and Cisco network devices. Aruba sets the keepalive packet's GRE protocol field to 0x801; however, Cisco sets the GRE protocol field to 0. When the cisco option is enabled, the Arubamanaged device automatically sets the GRE protocol value to 0.</p> <p>The <interval> option sets the number of seconds at which the keepalive frames are sent. Range is 1 second to 86400 seconds and default is 10 seconds.</p> <p>The <retries> option sets the number of consecutive times that the keepalives fail before the tunnel is considered to be down. Range is 0 to 1024 and default is 3.</p>
<pre>mode gre {ip ipv6 <num>}</pre>	<p>This parameter specifies the tunnel encapsulation method as GRE and allows you to specify whether it is a Layer-2 or Layer-3 GRE tunnel.</p> <ul style="list-style-type: none"> ■ ip: Specifies an IPv4 Layer-3 GRE tunnel. The protocol number is set to 0x0800 and is not configurable.

Parameter	Description
	<p>Traffic is redirected into the tunnel using a static route or a session ACL policy. The managed device encapsulates the Layer-3 packet only.</p> <ul style="list-style-type: none"> ■ ipv6: Specifies an IPv6 Layer-3 GRE tunnel. The protocol number is set to 0x86DD and is not configurable. Traffic is redirected into the tunnel using a static route or a session ACL policy. The managed device encapsulates the Layer-3 packet only. ■ <num>: A 16-bit protocol number that uniquely identifies a GRE tunnel. The number format is numeric. The managed devices at both endpoints of the tunnel must be configured with the same protocol number. The protocol number does not necessarily have to match the protocol number of the encapsulated frame. The managed device encapsulates the entire frame, including the

Parameter	Description
	Layer-2 header.
<pre> source controller-ip ipv6 {controller-ip loopback {vlan <vlanid>} <ipv6-addr>} loopback {vlan <vlanid>} <ip-addr> </pre>	<p>The local endpoint of the tunnel on the controller. This can be one of the following:</p> <ul style="list-style-type: none"> ■ controller-ip: IPv4 address of the managed device. ■ ipv6: Specify one of the following IPv6 options: <ul style="list-style-type: none"> ■ controller-ip: Specify the IPv6 address of the managed device. ■ loopback: Specify the IPv6 loopback interface configured on the managed device. ■ vlan <vlan -id>: Specify the VLAN interface ID. ■ <ipv6-addr>: Specify the IPv6 address. ■ loopback: Specify the loopback interface configured on the managed device. ■ vlan <vlanid>: Specify the VLAN interface ID. ■ <ip-addr>: Specify an IPv4 address.

Parameter	Description
<pre>vlan {add <word> remove <word> <word>}</pre>	<p>Specify the VLANs to be included in this tunnel.</p> <ul style="list-style-type: none"> ■ add <word>: The VLANs to be added to the current list. Separate the VLANs by a comma (,) ■ remove <word>: The VLANs to be removed from the current list. Separate the VLANs by a comma (,) ■ <word>: The VLANs that should be part of the current list. Separate the VLANs by a comma (,) <p>NOTE: You can configure a VLAN only if the tunnel mode is set to Layer-2 (mode gre <16-bit protocol number>). If the tunnel mode is not set to Layer-2 mode, the system displays an error message: <i>Tunnel is an IP [v6] GRE Tunnel. Change the mode before adding this.</i></p>

Examples

Layer-2 GRE Tunnel

The following CLI command configures a Layer-2 GRE tunnel:

MN-1 Configuration

```
(host) [mynode] (config)# interface tunnel 101
description "IPv4 Layer-2 GRE 101"
tunnel mode gre 1
tunnel source vlan 101
tunnel destination 192.168.1.1
tunnel keepalive
trusted
tunnel vlan 101
trusted vlan 101
```

MN-2 Configuration

```
(host) [mynode] (config)# interface tunnel 201
description "IPv4 Layer-2 GRE 201"
tunnel mode gre 1
tunnel source vlan 201
tunnel destination 192.168.2.1
tunnel keepalive
trusted
tunnel vlan 201
trusted vlan 201
```

IPv4 Layer-3 GRE Tunnel

The following CLI command examples configure a Layer-3 GRE tunnel for IPv4 between two managed devices.

MN-1 Configuration

```
(MN-1) (host) [mynode] (config) #interface tunnel 301
(host) [mynode] (config-submode) #description "IPv4 L3 GRE 301"
(host) [mynode] (config-submode) #tunnel mode gre ip
(host) [mynode] (config-submode) #ip address 192.1.1.1 255.255.255.255
(host) [mynode] (config-submode) #tunnel source vlan 301
(host) [mynode] (config-submode) #tunnel destination 20.20.20.249
(host) [mynode] (config-submode) #tunnel vlan 301
(host) [mynode] (config-submode) #trusted vlan 301
```

MN-2 Configuration

```
(MN-2) (host) [mynode] (config) #interface tunnel 401
(host) [mynode] (config-submode) #description "IPv4 L3 GRE 401"
(host) [mynode] (config-submode) #tunnel mode gre ip
(host) [mynode] (config-submode) #ip address 168.1.1.2 255.255.255.255
(host) [mynode] (config-submode) #tunnel source vlan 401
```

```
(host) [mynode] (config-submode) #tunnel destination 10.10.10.249
(host) [mynode] (config-submode) #tunnel vlan 401
(host) [mynode] (config-submode) #trusted vlan 401
```

IPv6 Layer-3 GRE Tunnel

The following CLI command examples configure a Layer-3 GRE tunnel for IPv6 between two managed devices.

MN-1 Configuration

```
(MN-1) (host) [mynode] (config) #interface tunnel 501
(host) [mynode] (config-submode) #description "IPv6 Layer-3 GRE 501"
(host) [mynode] (config-submode) #tunnel mode gre ipv6
(host) [mynode] (config-submode) #ip address 2001:1:2:1::1
(host) [mynode] (config-submode) #tunnel source vlan 501
(host) [mynode] (config-submode) #tunnel destination 2001:1:2:2020::1
(host) [mynode] (config-submode) #tunnel vlan 501
(host) [mynode] (config-submode) #trusted vlan 501
```

MN-2 Configuration

```
(MN-2) (host) [mynode] (config) #interface tunnel 601
(host) [mynode] (config-submode) #description "IPv6 Layer-3 GRE 601"
(host) [mynode] (config-submode) #tunnel mode gre ipv6
(host) [mynode] (config-submode) #ip address 2001:1:2:1::2
(host) [mynode] (config-submode) #tunnel source vlan 601
(host) [mynode] (config-submode) #tunnel destination 2001:1:2:1010::1
(host) [mynode] (config-submode) #tunnel vlan 601
(host) [mynode] (config-submode) #trusted vlan 601
```

Command History

Release	Modification
ArubaOS 8.5.0.0	The <code>keepalive icmp <ipaddr> <next-hop></code> parameter was introduced.
ArubaOS 8.4.0.0	Added the optional sub-parameters <code>vlan {add <word>} {remove <word>} <word></code> to the <code>trusted</code> parameter.
ArubaOS 8.2.0.0	Updated the new syntax as access group in <acl-name> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

interface vlan

```
interface vlan <vlan>
  bandwidth-contract <name>
  bcmc-optimization
  description <string>
  filter-broadcast-on-helper
  filter-broadcast-on-ipv6-helper
  ip
    access-group in <acl_name>
    address {<ipaddr> <ipmask>|dhcp-client client-id<cid>|internal|pppoe}
    helper-address <address>
    igmp {proxy {gigabitethernet <slot/module/port> | port-chanel <id>}}|snooping
    local-proxy-arp
    nat {inside|outside}
    ospf
      area
      authentication message-digest
      cost <value>
      dead-interval <1-65535>
      hello-interval <1-65535>
      message-digest-key <1 - 255> <passwd>
      priority <0-255>
      retransmit-interval <1-65535>
      transmit-delay <1-65535>
    pppoe-max-segment-size <mss>
    pppoe-password <password>
    pppoe-service-name <service-name>
    pppoe-username <username>
    pppoe-gateway-nat <nat-ip>
    routing
  ipv6
    address {dhcp6-client|link-local <ipv6-address>|pd <pd-
      name> ::X:X:X:X|<ipv6-prefix>/<prefix-length> eui-64}
    dhcp {pdclient <pd_name>|server <pool name>}
    helper-address <address>
    mld {proxy {gigabitethernet <slot/module/port>|port-chanel <id>}}|snooping
    nd
      ra {dns <ipv6_address>|dns-sl|enable|hop-limit <value>|interval
        <value>|life-time <value>|managed-config-flag|mtu <value>|other-config-
        flag|preference {high|low|medium}|prefix X:X:X:X::X/<0-128>}
      reachable-time <value>
      retransmit-time <value>
    ipv6-relay-option
    mtu <1280-1500>
    multimode-auth lease-time <5-3600>
    no ...
    operstate up
    option-82 {ap-name essid}|{mac [essid]}
    shutdown
    suppress-arp
```

Description

This command configures a VLAN interface. All ports on the managed device are assigned to VLAN 1 by default.

Parameter	Description
vlan	VLAN ID number. 1-4094
bandwidth-contract <name>	Name of the bandwidth contract to be applied to this VLAN interface. When applied to a VLAN, the contract limits both broadcast and multicast traffic. Use the <code>aaa bandwidth-contract</code> command to configure a bandwidth contract.
bcmc-optimization	Enables broadcast and multicast traffic optimization to prevent flooding of broadcast and multicast traffic on VLANs. If this feature is enabled on uplink ports, any managed device-generated Layer-2 packets will be dropped. disabled
description	String that describes this interface. 802.1q VLAN
filter-broadcast-on-helper	Filters DHCP discover broadcast when the helper is configured.
filter-broadcast-on-ipv6-helper	Filters DHCPv6 client multicast packets when the helper is configured.
ip	Configures IPv4 for this interface.
access-group in <acl_name>	Assigns an access list to inbound traffic on the interface, where <name> is the name of an access list. Routing ACL is the only supported ACL type that can be configured on a VLAN Interface. Other ACL types are not supported.
address	Configures the IP address for this interface, which can be one of the following: <ipaddr> <netmask> <ul style="list-style-type: none"> ▪ dhcp-client: use DHCP to obtain the IP address ▪ internal: IP address allocated from the branch group config. ▪ pppoe: use PPPoE to obtain the IP address
helper-address <address>	IP address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.

Parameter	Description
igmp	Enables IGMP proxy or IGMP snooping on this interface. See interface vlan ip igmp for complete details on this parameter.
local-proxy-arp	Enables local proxy ARP.
nat {inside outside}	Enables source NAT for all traffic routed from or to this VLAN. CAUTION: All ports on the managed device are assigned to VLAN 1 by default. Do not enable the nat inside option for VLAN 1, as this will prevent IPsec connectivity between the managed device and its IPsec peers.
ospf	Define an OSPF area. See interface vlan ip ospf for complete details on this parameter.
pppoe-max-segment-site	Configures the TCP MSS in bytes. 128
pppoe-password	Configures the PAP password on the PPPoE Access Concentrator for the switch. 1-80
pppoe-service-name	Configures the PPPoE service name. 1-80
pppoe-username	Configures the PAP username on the PPPoE Access Concentrator for the switch. 1-80
pppoe-gateway-nat <nat-ip>	Use the <nat-ip> sub-parameter to specify a NAT IP address instead of actual PPPoE gateway IP address to configure a default route.
routing	Enables layer-3 forwarding on the VLAN interface. To disable layer-3 forwarding, you must configure the IP address for the interface and specify no ip routing . enabled
ipv6	Configures IPv6 for this interface.
address	Configures the IPv6 address of interface. <ul style="list-style-type: none"> ▪ dhcp6-client - The DHCPv6 is used to obtain an IPv6 address. ▪ link-local - The link local address ▪ pd - The prefix obtained by PD client on uplink. ▪ X:X:X::X/<0-128> - The IPv6 prefix/prefix-length used to configure the global unicast address for

Parameter	Description
	this interface.
dhcp	Configures DHCP for IPv6. <ul style="list-style-type: none"> ▪ pdclient - The IPv6 prefix from a DHCPv6 Prefix delegation server. ▪ server - Configures the DHCPv6 pool for the vlan.
helper-address <address>	IPv6 address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.
mld	Enables MLD on this interface. <ul style="list-style-type: none"> ▪ proxy - Configures MLD proxy on the following interfaces. <ul style="list-style-type: none"> ▪ fastethernet ▪ gigabitethernet <slot/module/port> ▪ port-channel ▪ snooping - Configures the MLD snooping on this interface.
nd {ra reachable-time retransmit-time}	Configures the IPv6 neighbor discovery options. <ul style="list-style-type: none"> ▪ ra - configures the following router advertizement options: <ul style="list-style-type: none"> ◦ dns - Configures IPv6 recursive DNS server ◦ dns-sl - Configures IPv6 recursive DNS server search list ◦ enable - Enables IPv6 RA ◦ hop-limit - Configures RA hop-limit ◦ interval - Configures RA interval ◦ life-time - Configures RA lifetime ◦ managed-config-flag - Enables hosts to use DHCP server for stateful address autoconfiguration ◦ mtu - Configures MTU for RA ◦ other-config-flag - Enables hosts to use DHCP server for other non-address stateful autoconfiguration ◦ preference - Configures a router preference of high/low/medium ◦ prefix - Configures IPv6 RA prefix ▪ reachable-time - Configures neighbor discovery reachable time. By default this field is set to 0. Valid

Parameter	Description
	value - 0-3, 600,000 msec. ■ retransmit-time - Configures neighbor discovery retransmit time. By default this field is set to 0. Valid value - 0-3, 600,000 msec.
no	Negates any configured parameter.
ipv6-relay-option	Applies Relay-Option configuration to the DHCPv6 packets that need to be relayed from the WLAN interface.
mtu	MTU setting for the VLAN. 1024-1500
multimode-auth	MultiMode Authentication Support on VLAN
operstate up	Set the state of the interface to be up.
option-82 {ap-name [essid] mac [essid]}	Allows a DHCP relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server. The managed device, when acting as a DHCP relay agent, needs to be able to insert information about the AP and SSID through which a client is connecting into the DHCP request. Many service providers use this mechanism to make access control decisions. You can include: <ul style="list-style-type: none"> ■ AP name or AP name and ESSID. ■ MAC address or MAC address and ESSID.
shutdown	Causes a hard shutdown of the interface.
suppress-arp	Prevents flooding of ARP broadcasts on all the untrusted interfaces.

Example

The following example configures a VLAN interface:

```
(host) [mynode] (config) #interface vlan 16
(host) [mynode] (config-submode) #ip address 10.26.1.1 255.255.255.0
(host) [mynode] (config-submode) #ip helper-address 10.4.1.22
```

The following example displays the use of extended scope of address range:

```
(host) [mynode] (config) #interface vlan 214
(host) [mynode] (config-submode) #ipv6 address 2014::2/64
```



```
(host) [mynode] (config-submode) #ipv6 nd reachable-time 1000
(host) [mynode] (config-submode) #ipv6 nd retransmit-time 1000
(host) [mynode] (config-submode) #ipv6 nd ra enable
(host) [mynode] (config-submode) #ipv6 nd ra preference high
(host) [mynode] (config-submode) #ipv6 nd ra prefix 2014::/64
(host) [mynode] (config-submode) #operstate up
(host) [mynode] (config-submode) #ipv6 mld snooping
```

The following example configures DNS-SL on the VLAN interface:

```
(host) [md] (config) #interface vlan 1
(host) [md] (config-submode)#ipv6 nd ra dns-sl
abcdefghijklmnopqrstuvwxy123456
```

Related Commands

Command	Description
ip access-list route	This command configures an ACL for PBR.
ip nexthop-list	Use this command to define a next-hop list for a routing policy.
interface gigabitethernet	This command configures a GigabitEthernet interface and assigns a port to a configured VLAN.
show interface vlan	This command displays information about a specified VLAN interface.
show user	This command displays detailed information about user in terms of AP group, authentication method, role and so on

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>ipv6-relay-option</code> parameter was added.
ArubaOS 8.7.0.0	The <code>dns-sl</code> sub-parameter was added.
ArubaOS 8.4.0.0	The <code>pppoe-gateway-nat <nat-ip></code> sub-parameter was added.
ArubaOS 8.2.0.0	Updated the new syntax as access-group in <acl_name> . The following sub-parameters were introduced:

Release	Modification
	<ul style="list-style-type: none"> ▪ filter-broadcast-on-helper ▪ filter-broadcast-on-ipv6-helper ▪ ipv6 <helper-address>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

interface vlan ip igmp

```
interface vlan <vlan>
  ip igmp {proxy {gigabitethernet <slot/module/port>} | port-channel <id>} |
  snooping
```

Description

This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

The newer IGMP proxy feature and the older IGMP snooping feature cannot be enabled at the same time, as both features add membership information to multicast group table. For most multicast deployments, you should enable the IGMP Proxy feature on all VLAN interfaces to manage all the multicast membership requirements on the managed device. If IGMP snooping is configured on some of the interfaces, there is a greater chance that multicast information transfers may be interrupted.

This release of ArubaOS supports version 1 of the MLD protocol (MLDv1). MLDv1, defined in RFC 2710, is derived from version 2 of the IPv4 IGMPv2. You can use the command `interface vlan <vlan> ipv6 mld` to enable the MLD protocol and allow an IPv6 router to discover the presence of multicast listeners on directly-attached links. Use the CLI command `interface vlan <vlan> ipv6 mld snooping` for the Pv6 router to send multicast frames to only those nodes that need to receive them.

Parameter	Description
<code>proxy</code>	Enable IGMP proxy for this interface.
<code>gigabitethernet <slot/module/port></code>	Enable IGMP proxy on the specified GigabitEthernet (IEEE 802.3) interface.
<code>port-channel <id></code>	Enable IGMP proxy on the specified port channel.
<code>snooping</code>	Enable IGMP snooping. The IGMP protocol enables an router to discover the presence of multicast listeners on directly-attached links. Enable IGMP snooping to limit the sending of multicast frames to only those nodes that need to receive them.

Example

The following example configures IGMP proxy for vlan 2. IGMP reports from the managed device would be sent to the upstream router on gigabitethernet port 0/0/3.

```
(host) (conf)# interface vlan 2
```

```
(conf-subif)# ip igmp proxy gigabitethernet 0/0/3
```

Related Commands

Command	Description
interface vlan	Configure interface VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration VLAN Interface Mode (config-submode).

interface vlan ip ospf

```
interface vlan <vlan>
  ip ospf
    area
    authentication message-digest
    cost <cost>
    dead-interval <seconds>
    hello-interval <seconds>
    message-digest-key <keyid> <passwd>
    priority <number>
    retransmit-interval <seconds>
    transmit-delay <seconds>
```

Description

This command configures OSPF on the VLAN interface. When configuring OSPF over multiple vendors, use this command to ensure that all routers use the same cost. Otherwise, OSPF may route improperly.

Parameter	Description
area	Enable OSPF on a specific interface by entering the IP address of the router that will use OSPF.
authentication message-digest	Set the OSPF authentication mode to message digest. disabled
cost <cost>	Set the cost associated with the OSPF traffic on an interface. 1 to 65535 1
dead-interval <seconds>	Set the elapse interval (seconds) since the last hello-packet was received from the router. After the interval elapses, the neighboring routers declare the router dead. 1 to 65535 seconds 40
hello-interval <seconds>	Set the elapse interval (seconds) between hello packets sent on the interface. 1 to 65535 seconds 10
message-digest-key <keyid> <passwd>	Enable OSPF MD5 authentication and set the key identification and a character string password.

Parameter	Description
	<keyid> = 1 to 256 No default
priority <number>	Set the priority number of the interface to determine the designated router. 1 to 255 0
retransmit-interval <seconds>	Set the retransmission time between link state advertisements for adjacencies belonging to the interface. Set the time interval long enough to prevent unnecessary retransmissions. 1 to 65535 seconds 5
transmit-delay <seconds>	Set the elapse time before retransmitting link state update packets on the interface. 1 to 65535 seconds 5

Related Commands

Command	Description
interface vlan	Configures interface VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration VLAN Interface Mode (config-submode).

internal-modem

internal-modem
core-dump

Description

This command is used to configure the modem dump logs options.

Parameter	Description
core-dump	modem dump-logs generation to enable or disable.

Example

The following command enables modem dump-logs generation:

```
(host) [mynode] (config) #internal-modem core-dump
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Conductor.

iot-dev-upgrade

iot-dev-upgrade <ap-name> <device-mac>

Description

This command manually upgrades firmware on remote Aruba device.

Parameter	Description
<ap-name>	Name of the AP.
<device-mac>	Mac address of the AP.

Example

The following command manually upgrades firmware on remote Aruba device,

```
(host) [mm] iot-dev-upgrade ap-name ap-315 dev-mac 00:0f:1e:11:00:00
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

iot-manager

```
db-dump {im-db | im-log-db}
dp-optimize {im-db | im-log-db}
export ibeacon-info ap-group <ap-group>
replace-ap {old-ap-mac <old-ap-mac>} { new-ap-mac <new-ap-mac>}
```

Description

The IoT manager process interacts with the IoT database on the Mobility Conductor. Use this command to dump the content of the database to flash memory or repair the database and reclaim unused flash memory.

Parameter	Description
db-dump	This parameter instructs the mongo database to dump the content of the database to flash memory. This process can take time to complete and runs in the background while the command prompt returns.
im-db	This parameter instructs the mongo database to dump all content in the IoT manager database to flash memory.
im-log-db	This parameter instructs the mongo database to dump all content in the log database to flash memory.
dp-optimize	This parameter instructs the mongo database to repair the database and reclaim unused flash space. This process can take time to complete and runs in the background while the command prompt returns.
im-db	This parameter instructs the mongo database to repair all content in the IoT manager database and reclaim unused memory.
im-log-db	This parameter instructs the mongo database to repair all content in the log database and reclaim unused memory.
export ibeacon-info ap-group <ap-group>	This parameter export the iBeacon information of all devices in the specified AP group.
replace-ap	This parameter replaces an old AP of the specified BLE MAC address with a new AP of the specified BLE MAC address. The new AP inherits the ibeacon configuration of old AP.

Parameter	Description
old-ap-mac <old-ap-mac>	This parameter specifies the old AP with its BLE MAC address.
new-ap-mac <new-ap-mac>	This parameter specifies the new AP with its BLE MAC address.

Example

Access the CLI and use the following command to configure the IoT manager:

```
(host) [mynode] #iot-manager db-dump im-db
Dump process started at 2019-04-29 06:47:48. Dump file is im_db_dump.tgz.
Use 'show iot-manager debug db-dump-status' to check the status

(host) [mynode] #iot-manager db-optimize im-log-db
Optimize process started at 2019-04-30 08:57:18. Use 'show iot-manager debug
db-optimize-status' to check the status

(host) [mynode] #iot-manager export ibeacon-info ap-group default

(host) [mynode] #iot-manager replace-ap old-ap-mac 01:02:03:04:05:06 new-ap-
mac aa:ab:ac:ad:ae:af
```

Related Commands

Command	Description
show iot-manager	This command shows the status of the IoT manager.

Command History

Release	Modification
ArubaOS 8.7.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ export ■ replace-ap
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

iot radio-profile

```
iot radio-profile <profile-name>
  ble-console {dynamic|off|on}
  ble-opmode {beaconing|scanning}
  ble-txpower <ble-txpower>
  clone <source>
  no
  radio-instance {external | internal}
  radio-mode {ble | zigbee}
  zigbee-channel {auto|11|12|13|14|15|16|17|18|19|20|21|22|23|24|25|26}
  zigbee-opmode coordinator
```

Description

This command configures or modifies an IoT radio profile.

Parameter	Description
ble-console	Set the BLE console mode.
ble-opmode	Set the BLE operation mode.
ble-txpower	Set the BLE transmission power in dBm.
clone	Copy data from another IoT radio profile.
no...	Removes any existing configuration.
radio-instance	Enables external or internal radio instance.
radio-mode	Enables BLE or ZigBee radio mode.
zigbee-channel	Set the ZigBee scanning channel.
zigbee-opmode	Set the ZigBee coordinator operation mode.

Example

The following example configures an IoT transport profile.

```
(host) [mynode] (config) #iot radio-profile Sample-Zigbee
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #radio-mode zigbee
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #zigbee-channel auto
(host) [mynode] (IoT Radio Profile "Sample-Zigbee") #zigbee-opmode
coordinator
```

Related Commands

Command	Description
<code>show iot radio-profile</code>	Shows the IoT radio profile status.

Command History

Version	Modification
ArubaOS 8.6.0.0	<p>The following parameters were removed:</p> <ul style="list-style-type: none"> ▪ <code>radio-enable</code> ▪ <code>zigbee-panid</code> ▪ <code>zigbee-panid-type</code> ▪ <code>zigbee-permit joining</code> ▪ <code>zigbee-permit-joining-duration</code> <p>The following parameters were introduced:</p> <ul style="list-style-type: none"> ▪ <code>ble-console</code> ▪ <code>ble-opmode</code> ▪ <code>ble-txpower</code>
ArubaOS 8.4.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

iot-sniffer radio

```
iot-sniffer radio <radio_macaddr> {disable | enable | reset | start | stop}
```

Description

This command configures the IoT sniffer function on the radio of an AP.

Parameter	Description
<code><radio_macaddr></code>	<p>The MAC address of the radio on which the IoT sniffer function is configured. Available options are:</p> <ul style="list-style-type: none"> ▪ disable—Disables the IoT sniffer function.

Parameter	Description
	<ul style="list-style-type: none"> ▪ enable—Enables the IoT sniffer function. ▪ start—Starts capturing the packets based on the following parameters: <ul style="list-style-type: none"> ◦ server—Denotes the IPv4 server IP address or hostname. ◦ port—Denotes the UDP port number. ◦ zigbee-channel—Denotes the zigbee channel ID. Enter a value between 11 to 26. ▪ stop—Stops capturing the packets. ▪ reset—Resets the IoT sniffer function. Use this option if the IoT sniffer function is not working properly or to clear the configuration on the sniffer.

Example

The following example configures an IoT sniffer on the radio:

```
(host) [mynode] #iot-sniffer radio 90:4c:81:b2:81:f0 enable
```

Related Commands

Command	Description
show ap debug iot-sniffer	Shows the IoT sniffer information on the AP.

Command History

Version	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

iot transportProfile

```
iot transportProfile <profile>
  accessID <accessID>
  accessToken <token>
  ageFilter
  authentication-mode {client-credentials|none|password}
  authentication URL
  azure-dps-auth-type group-enrollment symmetric-key <key>
  azure-dps-id-scope
  bleDataForwarding
  blePeriodicTelemetryDisable
  cellSizeFilter
  cipher-list
  client-secret
  clientID <id>
  clone
  companyIdentifierFilter <filter>
  customFadingFactor
  dataFilter <dataFilter>
  deviceClassFilter {abilitySmartSensor|all|aruba-beacons|aruba-sensors|aruba-
tags|assa-abloy|eddytone|enocan-sensors|enocan-switches|exposure-
notification|google|ibeacon|minew|mysphera|sbeacon|serial-data|unclassified|wifi-
assoc-sta|wifi-tags|wifi-unassoc-sta|wiliot|zf-tags|ZSD}
  deviceCountOnly
  environmentType {auditorium|custom|office|outdoor|shipboard|warehouse}
  include-ap-group
  localNameFilter <filter>
  macOuiFilter <filter>
  movementFilter <threshold>
  no
  password <password>
  perFrameFiltering
  proxy {server <servernm> port <portnum> |user <usernm> password <passwd>}
  reportingInterval <interval>
  rssiReporting
  rtlsDestMac <rtlsDestMac>
  serverType {Assa-Abloy | Azure-IoTHub | Meridian-Asset-Tracking | Meridian-
Beacon-Management | Telemetry -Https | Telemetry-Websocket}
  serverURL <url>
  serviceUUIDFilter <filter>
  uidNamespaceFilter
  urlFilter
  username <user>
  uuidFilter <filter>
  usbSerialDeviceTypeFilter <filter>
  vendorFilter
  ZSDFilter
```

Description

This command configures or modifies an IoT transport profile. An IoT transport profile is a global profile that is used to transport BLE information to an endpoint server.



In some cases, the iot transport profile having a serverType that is supported from ArubaOS 8.4.0.0 version onwards will be skipped when downgrading to a previous version. In such cases, the default serverType will be applied. The default serverType applied might not be a valid serverType that corresponds with other parameters configured in the iot transport profile. The operator must manually fix the configuration parameters in the iot transport profile to match the serverType.

Parameter	Description
<code>accessID <accessID></code>	An access ID will grant extended access. Applies only to endpoint type Assa-Abloy.
<code>accessToken <accessToken></code>	Access token. Configure this only if you want to bypass authentication.
<code>ageFilter</code>	Age filter. Devices without recent activity will not be reported.
<code>authentication-mode</code>	Authentication mode to use with authentication server. Available options are: <ul style="list-style-type: none">▪ client-credentials - Use credentials of the client▪ none - Do not use any credentials▪ password - Use password as credentials
<code>authenticationURL <url></code>	Server URL for authentication.
<code>azure-dps-auth-type group-enrollment symmetric-key <key></code>	Symmetric key to enroll devices in a group on the Azure DPS.
<code>azure-dps-id-scope</code>	Azure DPS ID scope for device provisioning.
<code>bleDataForwarding</code>	Enables BLE data forwarding for known devices.
<code>blePeriodicTelemetryDisable</code>	Disable periodic telemetry report.

Parameter	Description
	<p>NOTE: This command only works for telemetry-websocket Server Type.</p>
cellSizeFilter	<p>A proximity filter. Devices outside the cell will not be reported. Size is specified in meters. Setting to 0 disables the cell size filter.</p>
cipher-list	<p>Cipher list to be used for connections between IOT transport profile and third party server.</p>
client-secret	<p>Password to use when authenticating using client credentials.</p>
clientId <id>	<p>This ID identifies the sender to the server.</p>
clone	<p>Copy data from another IoT data profile.</p>
companyIdentifierFilter <filter>	<p>This is a 2-bytes integer, for example, "HPE - 0x011B" or "Wiliot - 0x0500". You can also include an extra byte which indicates the next layer type, like for HPE - 0x011B, 0x08, which means that the device type used is Aruba sensors.</p>
customFadingFactor	<p>When environment type is custom, you can define a fading factor to get the most accurate distance according to your environment.</p> <p>10-40</p>
dataFilter <dataFilter>	<p>A list of numbers to filter the data before reporting to a server. The numbers correspond to protobuf files. For dataFilter values, see DataFilter Values.</p>

Parameter	Description
deviceClassFilter <device>	A list of device class tags to filter the devices included in the reports. You can specify a maximum of 10 device classes.
abilitySmartSensor	ABB ability smart sensor data
all	All BLE data
aruba-beacons	Aruba beacon data
aruba-sensors	Aruba sensor data
aruba-tags	Aruba tag data
assa-abloy	Assa Abloy door lock data
eddystone	Eddystone data
enoccean-sensors	EnOcean sensor data
enoccean-switches	EnOcean switch data
exposure-notification	Exposure notification based on the presence of service UUID 0xFD6F and service data 0xFD6F
google	Google sensor data
ibeacon	iBeacon data
minew	Minew data
mysphera	MySphera data
sbeacon	Sbeacon data
serial-data	Serial data
unclassified	Unclassified data
wifi-assoc-sta	Data of WiFi associated stations
wifi-tags	WiFi RTLS tag data

Parameter	Description
wifi-unassoc-sta	Data of WiFi unassociated stations
wiliot	Wiliot data
zf-tags	ZF tag data
ZSD	ZigBee Socket Device
deviceCountOnly	Send only the aggregated device counts per configured device class
environmentType	Configure the working environment type.
auditorium	Configure the working environment type as auditorium.
custom	Configure a custom working environment type. Optionally, configure customFadingFactor.
office	Configure the working environment type as office.
outdoor	Configure outdoor working environment type.
shipboard	Configure the working environment type as shipboard.
warehouse	Configure the working environment type as warehouse.
include-ap-group	Configure AP groups that use the transport profile.
localNameFilter <filter>	It is a string, that can do string matching. It matches both advertisement and scan response.

Parameter	Description
<code>macOuiFilter <filter></code>	It is a 3 bytes array. Only public MAC address(non-randomized) are considered. For example, 60:C0:BF is MAC OUI of Blyott devices.
<code>movementFilter <threshold></code>	Filters devices that do not change distance. Specified in meters. Applicable only if a cell size is set. Setting to 0 disables the movement filter.
<code>no</code>	Removes any existing configuration.
<code>password <password></code>	Password for authentication.
<code>perFrameFiltering</code>	Applies transport profile filters to each frame rather than on the device. This parameter can be enabled only when the parameter <code>bleDataForwarding</code> is enabled. This parameter is ignored when the parameter <code>bleDataForwarding</code> is disabled. This parameter is disabled by default.
<code>proxy</code>	Information of the proxy server to which the IoT data is sent.
<code>server <servernm> port <portnum></code>	IP address and port number of the proxy server.
<code>user <usernm> password <passwd></code>	Username and password to log in to the proxy server. This parameter is optional.
<code>reportingInterval<interval></code>	Reporting interval in seconds. 5 to 3600 seconds

Parameter	Description
<code>rssiReporting <format></code>	Set the preferred format for RSSI reporting.
<code>average</code>	RSSI averaged over the reporting period
<code>bulk</code>	RSSI Bulk
<code>last</code>	Most Recent RSSI
<code>max</code>	Maximum RSSI measured over the reporting period
<code>smooth</code>	Smoothed RSSI measured over the reporting period
<code>rtlsDestMAC</code>	Set the destination MAC address filter for RTLS tags.
<code>serverType <type></code>	The type of server that is receiving the telemetry stream.
<code>Assa-Abloy</code>	Stream data to Assa Abloy Visionline server.
<code>Azure-IoTHub</code>	Stream data to Azure IoT hub.
<code>Meridian-Asset-Tracking</code>	Stream data to Meridian websocket server.
<code>Meridian-Beacon-Management</code>	POST data to a RESTful Meridian API.
<code>Telemetry-Https</code>	POST data to a RESTful Aruba API.
<code>Telemetry-Websocket</code>	Stream data to a websocket based server.
<code>serverURL <url></code>	Server URL for sending telemetry.
<code>serviceUUIDFilter <filter></code>	It is a 2 bytes integer, and it could be more than one entry. For example, 0x180F is SIG-adopted service UUID.

Parameter	Description
<code>uidNamespaceFilter</code>	A list of UID namespaces to filter devices included in the reports. Applies only Eddystone-UID devices. You can specify a maximum of 10 namespaces.
<code>urlFilter</code>	A list of URL strings to filter devices included in the reports. Applies only Eddystone-URL devices. The string listed here can be partial URL strings. You can specify a maximum of 10 URL strings.
<code>username <user></code>	Username for authentication.
<code>uuidFilter <filter></code>	A list of UUIDs to filter the devices included in the reports. Applies only to iBeacon devices. You can specify a maximum of 10 UUIDs.
<code>usbSerialDeviceTypeFilter <filter></code>	Enables the use to filter serial data based on the USB serial dongle type. The following serial data type can be filtered: <ul style="list-style-type: none"> ▪ EnOcean ▪ OSU ▪ Piera
<code>vendorFilter</code>	A list of list of vendor IDs and vendor names. You can specify a maximum of 5 vendor IDs or vendor names.
<code>ZSDFilter</code>	A list of ZSD to filter the zigbee socket devices.

DataFilter Values

Value	Description
#2	reporter
2.1	name
2.3	ipv4
2.4	ipv6
2.5	hwType
2.6	swVersion
2.7	swBuild
2.8	time
#3	reported
3.2	deviceClass
3.3	model
3.4	firmware
3.5	assetId
3.6	publicKey
3.7	lastSeen
3.9	bevent
3.10	rssi
3.11	cell
3.12	beacons
3.13	txpower
3.14	sensors
3.14.1	accelerometer
3.14.2	battery
3.14.3	temperatureC
3.14.4	humidity
3.14.5	voltage

Value	Description
3.14.6	illumination
3.14.7	motion
3.14.8	current
3.14.9	CO
3.14.10	CO2
3.14.11	VOC
3.14.12	resistance
3.14.13	pressure
3.14.14	alarm
3.14.15	contact
3.14.16	occupancy
3.14.17	mechanicalHandle
3.14.18	distance
3.14.19	capacitance
3.16	stats
3.16.1	uptime
3.16.2	adv_cnt
3.16.3	seq_nr
3.17	inputs
3.18	vendorData
3.19	vendorName
3.20	sensorTimestamp
3.21	flags
3.22	localName
3.23	identity

Example

The following example configures an IoT transport profile.

```
(host) [mynode] (config) #iot transportProfile sample
(host) [mynode] (IoT Data Profile "sample") #serverURL
https://edit.meridianapps.com/api/beacons/manage
(host) [mynode] (IoT Transport Profile "sample") #serverType Meridian-
Beacons-Management
(host) [mynode] (IoT Transport Profile "sample") #deviceClassFilter managed-
beacons
(host) [mynode] (IoT Transport Profile "sample") #reportingInterval 300
(host) [mynode] (IoT Transport Profile "sample") #accessToken
MzkxMTZlMWYtYTgzYS00YWUxLTkzYWEtYjQyNzE1MGM5MjAxOjBiZWJjYWViLTRjNjItNGEwNC1h
MGIyLWYzZTM5ZDF1NGVknG==
```

Related Commands

Command	Description
iot usetransportProfile	Sets an IoT management server profile.
show iot transportProfile	Shows the IoT profile status.

Command History

Release	Modification
ArubaOS 8.9.0.0	<p>The following parameters were introduced:</p> <ul style="list-style-type: none">■ usbSerialDeviceTypeFilter <filter>■ companyIdentifierFilter <filter>■ serviceUUIDFilter <filter>■ macOuiFilter <filter>■ localNameFilter <filter> <p>The server-type ZF-Openmatics parameter was removed.</p>
ArubaOS 8.8.0.0	<p>The following parameters were introduced:</p> <ul style="list-style-type: none">■ azure-dps-auth-type group-enrollment symmetric-key■ azure-dps-id-scope■ authentication-mode■ client-secret■ bleDataForwarding■ perFrameFiltering <p>The following deviceClassFilters were introduced:</p>

Release	Modification
	<ul style="list-style-type: none"> ▪ google ▪ minew <p>The Azure-IoTHub server type was introduced.</p>
ArubaOS 8.7.0.0	<p>The following parameters were introduced:</p> <ul style="list-style-type: none"> ▪ <code>ZSDFilter</code> ▪ <code>dataFilter</code> <p>The following deviceClassFilter were introduced:</p> <ul style="list-style-type: none"> ▪ exposure-notification ▪ serial-data ▪ wiliot ▪ ZSD <p>The enableOnController parameter was removed.</p>
ArubaOS 8.6.0.0	<p>The following parameters were introduced:</p> <ul style="list-style-type: none"> ▪ <code>deviceCountOnly</code> ▪ <code>proxy</code> ▪ <code>rtlsDestMAC</code> ▪ <code>vendorFilter</code> <p>The following deviceClassFilters were introduced:</p> <ul style="list-style-type: none"> ▪ abilitySmartSensor ▪ mysphera ▪ sbeacon ▪ wifi-assoc-sta ▪ wifi-tags ▪ wifi-unassoc-sta
ArubaOS 8.5.0.0	<p>Added the <code>aruba-sensors</code> sub-parameter to the <code>deviceClassFilter</code> parameter.</p>
ArubaOS 8.4.0.0	<p>The following server types were introduced:</p> <ul style="list-style-type: none"> ▪ Meridian-beacons-management ▪ Meridian-asset-tracking ▪ Telemetry-https ▪ Telemetry-websocket ▪ ZF-openmatics <p>The following deviceClassFilters were introduced:</p> <ul style="list-style-type: none"> ▪ all ▪ aruba-beacons ▪ aruba-tags ▪ eddystone ▪ enoccean-sensors ▪ enoccean-switches ▪ ibeacon ▪ unclassified

Release	Modification
	<ul style="list-style-type: none"> ▪ zf-tags <p>The following parameters were renamed from:</p> <ul style="list-style-type: none"> ▪ endpointType to serverType ▪ endpointID to clientID ▪ endpointURL to serverURL ▪ endpointToken to accessToken ▪ transportInterval to reportingInterval ▪ payloadContent to deviceClassFilter ▪ filterAttribute to uuidFilter ▪ namespaceFilter to uidNamespaceFilter ▪ cellSize to cellSizeFilter ▪ thresholdAttribute to movementFilter ▪ outrangeAgeout to ageFilter
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

iot usetransportProfile

```
iot usetransportProfile <iot-profile-name>
```

Description

This command sets an IoT management server profile. You can set up to four management server profiles.

Example

Execute the following command to set an IoT transport profile:

```
(host) [mynode] (config)# iot usetransportProfile sample
```

Related Commands

Command	Description
iot transportProfile	Configures an IoT transport profile.
show iot transportProfile	Shows the IoT profile status.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

ip access-list eth

```
ip access-list eth <accname>
deny {<ethertype> [<bits>]|any} [mirror] [position <prio>]
no ...
permit {<ethertype> [<bits>]|any} [mirror] [position <prio>]
```

Description

This command configures an Ethertype ACL. The Ethertype field in an Ethernet frame indicates the protocol being transported in the frame. This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. This ACL can be used to permit IP frames while blocking other non-IP protocols such as IPX or Appletalk.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see [firewall on page 636](#).

Parameter	Description
<accname>	Define an access list, where <accname> is a name, or a number in the specified range. 200-299
deny	Reject the specified packets, which can be one of the following: <ul style="list-style-type: none">▪ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535)▪ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination, or set the position of the ACL. The default position is last, a position of 1 puts the ACL at the top of the list.
no	Negates any configured parameter.
permit	Allow the specified packets, which can be one of the following: <ul style="list-style-type: none">▪ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535)▪ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination, or set the position of the ACL. The default position is last, a position of 1 puts the ACL at the top of the list.

Example

The following command configures an Ethertype ACL:

```
(host) [mynode] (config) #ip access-list eth 200
(host) [mynode] (config-submode)#permit any mirror position 3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list extended

```
ip access-list extended <accname>
  deny <protocol> <source> <dest>
  ipv6 <protocol> <source> <dest>
  no ...
  permit <protocol> <source> <dest>
```

Description

This command configures an extended ACL. To configure IPv6 specific rules, use the **ipv6** keyword for each rule.

Extended ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source or destination IP address or IP protocol.

Parameter	Description
extended <accname>	Define an access list, where <accname> is a name, or a number in the specified range. 100-199, 2000-2699
deny	Reject the specified packets.
<protocol>	Protocol, which can be one of the following: <ul style="list-style-type: none">▪ any: any protocol▪ icmp: Internet Control Message Protocol▪ igmp: Internet Gateway Message Protocol▪ tcp: Transmission Control Protocol▪ udp: User Datagram Protocol▪ <0-255>: An IP protocol number between 0-255
<source>	Source, which can be one of the following: <ul style="list-style-type: none">▪ any: any source▪ host: specify a single host IP address▪ A.B.C.D: IPv4 source address and wildcard
<dest>	Destination, which can be one of the following: <ul style="list-style-type: none">▪ any: any destination▪ host: specify a single host IP address▪ A.B.C.D: IPv4 destination address and wildcard
ipv6 <deny permit>	Use the ipv6 keyword to add IPv6 specific rules.
<protocol>	Protocol, which can be one of the following: <ul style="list-style-type: none">▪ any: any protocol▪ icmpv6: Internet Control Message Protocol▪ tcp: Transmission Control Protocol

Parameter	Description
	<ul style="list-style-type: none"> ▪ udp: User Datagram Protocol ▪ <0-255>: An IP protocol number between 0-255
<source>	Source, which can be one of the following: <ul style="list-style-type: none"> ▪ any: any source ▪ host: specify a single host IP address ▪ X:X:X:X:/<0-128>: IPv6 source address and wildcard
<dest>	Destination, which can be one of the following: <ul style="list-style-type: none"> ▪ any: any destination ▪ host: specify a single host IP address ▪ X:X:X:X:/<0-128>: IPv6 destination address and wildcard
no	Negates any configured parameter.
permit	Allow the specified packets.
<protocol>	Protocol, which can be one of the following: <ul style="list-style-type: none"> ▪ any: any protocol ▪ icmp: Internet Control Message Protocol ▪ igmp: Internet Gateway Message Protocol ▪ tcp: Transmission Control Protocol ▪ udp: User Datagram Protocol ▪ <0-255>: An IP protocol number between 0-255
<source>	Source, which can be one of the following: <ul style="list-style-type: none"> ▪ any: any source ▪ host: specify a single host IP address ▪ A.B.C.D: IPv4 source address and wildcard
<dest>	Destination, which can be one of the following: <ul style="list-style-type: none"> ▪ any: any destination ▪ host: specify a single host IP address ▪ A.B.C.D: IPv4 destination address and wildcard

Example

The following command configures an extended ACL:

```
(host) [mynode] (config) #ip access-list extended 100
(host) [mynode] (config-submode) #deny any host 1.1.21.245 any
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list geolocation

```
ip access-list geolocation global-geolocation-acl
deny
{[<from>|<to> {anonymous_proxy [log|mirror|position]|any
[log|mirror|position]}|country <STRING>|region <STRING>}]
no ...
permit
{[<from>|<to> {anonymous_proxy [log|mirror|position]|any
[log|mirror|position]}|country <STRING>|region <STRING>}]
```

Description

This command configures a global geolocation ACL.

Parameter	Description
deny <from to>	Reject the specified packets, which can be one of the following: <ul style="list-style-type: none">▪ Packets coming from the source.▪ Packets meant for the destination.
anonymous_proxy <log mirror position>	Match packets from or to an anonymous proxy. It has the following options: <ul style="list-style-type: none">▪ Log if the ACL is applied.▪ Mirror all session packets to datapath or remote destination.▪ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
any <log mirror position>	Match any location. It has the following options: <ul style="list-style-type: none">▪ Log if the ACL is applied.▪ Mirror all session packets to datapath or remote destination.▪ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
country <STRING>	Match packets from or to a country. The <STRING> denotes country name. NOTE: Use double quotes to specify country names with spaces in the name.

Parameter	Description
<code>region <STRING></code>	<p>Match packets from or to a region. Region denotes the name of a continent and it should be entered in lower-case. Refer the following examples to mention the region string:</p> <ul style="list-style-type: none"> ▪ <code><africa></code> ▪ <code><north-america></code> ▪ <code><south-america></code> ▪ <code><europe></code> ▪ <code><asia></code> ▪ <code><australia></code>
<code>no</code>	<p>Negates any configured parameter.</p>
<code>permit <from to></code>	<p>Allow the specified packets, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ Packets coming from the source. ▪ Packets meant for the destination.
<code>anonymous_proxy <log mirror position></code>	<p>Match packets from or to an anonymous proxy. It has the following options:</p> <ul style="list-style-type: none"> ▪ Log if the ACL is applied. ▪ Mirror all session packets to datapath or remote destination. ▪ Filter position. The position number is in the range of <code><1-2000></code>. The default is last, and 1 is first position.
<code>any <log mirror position></code>	<p>Match any location. It has the following options:</p> <ul style="list-style-type: none"> ▪ Log if the ACL is applied. ▪ Mirror all session packets to datapath or remote destination. ▪ Filter position. The position number is in the range of <code><1-2000></code>. The default is last, and 1 is first position.
<code>country <STRING></code>	<p>Match packets from or to a country. The <code><STRING></code> denotes country name.</p> <p>NOTE: Use double quotes to specify country names with spaces in the name.</p>
<code>region <STRING></code>	<p>Match packets from or to a region. The <code><STRING></code> denotes region name. Match packets from or to a region. The <code><STRING></code> denotes the name of a continent and it should be entered in lower-case. Refer the following examples to mention the region string:</p> <ul style="list-style-type: none"> ▪ <code><africa></code>

Parameter	Description
	<ul style="list-style-type: none"> ▪ <north-america> ▪ <south-america> ▪ <europe> ▪ <asia> ▪ <australia>

Example

The following command configures a geolocation ACL:

```
(host) [mynode] (config) #ip access-list geolocation global-geolocation-acl
(host) [mynode] (config-submode)#permit from any mirror position 3
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list mac

```
ip access-list mac <accname>
  deny {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
  no ...
  permit {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
```

Description

This command configures a MAC ACL. MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses. If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see [firewall on page 636](#).

Parameter	Description
mac <accname>	Configures a MAC access list, where <accname> is a name, or a number in the specified range. 700-799, 1200-1299
deny	Reject the specified packets, which can be the following: <ul style="list-style-type: none">▪ any: any packets▪ host: specify a MAC address▪ A:B:C:D:E:F: MAC address and optional wildcard Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.
no	Negates any configured parameter.
permit	Allow the specified packets, which can be the following: <ul style="list-style-type: none">▪ any: any packets▪ host: specify a MAC address▪ A:B:C:D:E:F: MAC address and optional wildcard Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.

Example

The following command configures a MAC ACL:

```
(host) [mynode] (config) #ip access-list mac 700
(host) [mynode] (config-submode) #deny 11:11:11:00:00:00
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list route

```
ip access-list route <accname>
  <source> <dest> <service> <action> forward|route {ipsec-map <ipsec-map-name>}|
  {next-hop-list <next-hop-list-name>}|{tunnel <tunnel-id>}|{tunnel-group
  <tunnelgroupname>} [position <position>]
  ipv6 <source> <dest> <service> <action> forward|route > {next-hoplist <next-hop-
  list-name>} [position <position>]
no ...
```

Description

This command configures an ACL for PBR.

PBR is an optional feature that allows packets to be routed based on ACLs configured by the administrator. By default, when a managed device receives a packet for routing, it looks up the destination IP in the routing table and forwards the packet to the nexthop router. If PBR is configured, the nexthop device can be chosen based on a defined ACL.

In a typical deployment scenario with multiple uplinks, the default route only uses one of the uplink next-hops for forwarding packets. If a nexthop becomes unreachable, the packets will not reach their destination. If your deployment uses PBR based on a nexthop list, any of the uplink nexthops could be used for forwarding traffic. This requires a valid ARP entry (Route-cache) in the system for all the PBR nexthops.



IPv6 PBR does not support WAN uplink functionality.

Parameter	Description
route <accname>	Define a route access list, where <accname> is an access list name
<source>	The traffic source, which can be one of the following: <ul style="list-style-type: none">▪ alias<name>: specify the network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases)▪ any: match any traffic▪ description: brief description about this route acl (up to 128 characters in quotes)▪ host <ip-addr>: specify a single host IP address▪ localip: specify the local IP address to match traffic▪ network <ip-addr> <netmask>: specify the IP address and netmask▪ no: negate a command▪ user: represents the IP address of the user

Parameter	Description
	<p>NOTE: Only any, host <ip-addr>, and network <ip-addr> <netmask> options are supported for IPv6 address.</p> <p>NOTE: You cannot configure IPv6 multicast, link-local, unspecified, loopback, and subnet anycast addresses as IPv6 source addresses.</p>
<dest>	<p>The traffic destination, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ alias<name>: specify the network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases) ▪ any: match any traffic ▪ description: brief description about this route acl (up to 128 characters in quotes) ▪ host <ip-addr>: specify a single host IP address ▪ localip: specify the local IP address to match traffic ▪ network <ip-addr> <netmask>: specify the IP address and netmask ▪ user: represents the IP address of the user <p>NOTE: Only any, host <ip-addr>, and network <ip-addr> <netmask> configuration options are supported for IPv6 address.</p> <p>NOTE: You cannot configure IPv6 multicast, link-local, unspecified, loopback, and subnet anycast addresses as IPv6 destination addresses.</p>
<service>	<p>Network service to which the ACL is applied. The service can be one of the following:</p> <ul style="list-style-type: none"> ▪ any: match any traffic ▪ app<string>: application name. (For a complete list of supported applications, issue the command show dpi application all.) ▪ appcategory <string>: application category name. (For a complete list of supported applications, issue the command show dpi application all.) ▪ icmp: Internet Control Message Protocol ▪ tcp <0-65535>: specify the TCP destination port number (0-65535) ▪ tcp source<0-65535>: TCP source port number ▪ udp <0-65535>: UDP destination port number (0-65535) ▪ udp source<0-65535>: UDP source port number

Parameter	Description
	<ul style="list-style-type: none"> ▪ <0-255>: IP protocol number (0-255) ▪ <string>: name of a network service (use the show netservice command to see configured services) <p>NOTE: Only any configuration option is supported for IPv6 address.</p>
<action>	<p>Action if rule is applied, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ forward: Explicitly define an ACL with a forward action to skip PBR for traffic which would otherwise match another PBR rule. ▪ route ipsec-map <ipsec-map-name>: Redirected over a VPN tunnel by specifying the ipsec-map name. For more information on IPsec maps, see crypto-local ipsec-map. ▪ route next-hop-list <next-hop-list-name>: Packets can be routed to a nexthop router on a nexthop list by specifying the nexthop list name. For more information on nexthop lists, see ip nexthop-list. ▪ route tunnel <tunnel-id>: Packets can be redirected over an L3 GRE tunnel. ▪ route tunnel-group <tunnelgroupname>: Packets can be redirected over an L3 GRE tunnel group. For more information on tunnel groups, see tunnel-group. ▪ [position <position>]: (Optional) Specify the position of the forwarding or routing rule. (1 is first, default is last) <p>NOTE: Only route next-hop-list <next-hop-list-name> configuration option is supported for IPv6 address.</p>

Example

The following command configures a routing access list using an IPsec map.

```
(host) [mynode] (config) #ip access-list route pbr1
(host) [mynode] (config-submode) #any any udp 100 route ipsec-map VPN1
```

The following command configures IPv6 rules in routing access list using next-hop list:

```
(host) [mynode] (config) #ip access-list route pbr2
(host) [mynode] (config-submode) #ipv6 any any any route next-hop-list new
```



A PBR ACL can have both IPv4 and IPv6 rules.

Related Commands

Command	Description
interface vlan	This command associates a routing ACL with a specific VLAN.
ip nexthop-list	This command defines a next-hop list for IPv4 address in policy-based routing.
ipv6 nexthop-list	This command defines a next-hop list for IPv6 address in policy-based routing.

Command History

Release	Modification
ArubaOS 8.8.0.0	A new sub-parameter is added to capture a brief description of the route ACL.
ArubaOS 8.6.0.0	The following configuration options were included under <code>ipv6</code> parameter: <ul style="list-style-type: none">▪ any▪ host <ip-addr>▪ network<ip-addr><netmask>▪ route next-hop-list <next-hop-list-name>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list session

```
ip access-list session <accname>  
  <source> <dest> <service> <action> [<extended action>]  
  ipv6 <source> <dest> <service> <action> [<extended action>]  
no ...
```

Description

This command configures an ACL session. To create IPv6 specific rules, use the **ipv6** keyword. Session ACLs define traffic and firewall policies on the managed device. You can configure multiple rules for each policy, with rules evaluated from top (1 is first) to bottom. The first match terminates further evaluation. Generally, you should order more specific rules at the top of the list and place less specific rules at the bottom of the list. The ACL ends with an implicit deny all. To configure IPv6 rules, use the `ipv6` keyword followed by the regular ACL keywords.

Parameter	Description
<code>session <accname></code>	Define a session ACL, where <accname> is an access list name, or an access list number in the specified range.
<code>description</code>	Brief description about this session ACL (up to 128 characters in quote)
<code>ipv6</code>	Use the <code>ipv6</code> keyword to create IPv6 specific rules.
<code><source></code>	The traffic source, which can be one of the following: <ul style="list-style-type: none">▪ alias: specify the network resource (use the <code>netdestination</code> command to configure aliases; use the <code>show netdestination</code> command to see configured aliases)▪ any: match any traffic▪ description: brief description about this session acl (up to 128 characters in quotes)▪ host: specify a single host IP address▪ ipv6: specify a single host IPv6 address▪ localip: specify the local IP address to match traffic▪ network: specify the IP address and netmask▪ user: represents the IP address of the user▪ userrole: represents the traffic based on user role
<code><dest></code>	The traffic destination, which can be one of the following: <ul style="list-style-type: none">▪ alias: specify the network resource (use the <code>netdestination</code> command to configure aliases; use the <code>show netdestination</code> command to see configured aliases)

Parameter	Description
	<ul style="list-style-type: none"> ▪ any: match any traffic ▪ description: brief description about this session acl (up to 128 characters in quotes) ▪ host: specify a single host IP address ▪ ipv6: specify a single host IPv6 address ▪ localip: specify the local IP address to match traffic ▪ network: specify the IP address and netmask ▪ user: represents the IP address of the user ▪ userrole: represents the traffic based on userrole
<service>	<p>Network service, which can be one of the following:</p> <ol style="list-style-type: none"> 1. IP protocol number (0-255) 2. name of a network service (use the show netservice command to see configured services) 3. any: match any traffic 4. app: application name. (For a complete list of supported applications, issue the command <code>show dpi application all.</code>) 5. appcategory: application category name. (For a complete list of supported applications, issue the command <code>show dpi application all.</code>) 6. icmp: Internet Control Message Protocol 7. tcp destination port number: specify the TCP port number (0-65535) 8. tcp source: TCP/UDP source port number 9. udp: specify the UDP port number (0-65535) 10. web-cc-category: name of a web content category. For the full list of available web content categories, issue the command show web-cc categories. 11. web-cc-reputation: any of the following predefined web content reputation levels: <ul style="list-style-type: none"> ▪ high-risk ▪ low-risk ▪ moderate-risk ▪ suspicious ▪ trustworthy
<action>	<p>Action if rule is applied, which can be one of the following:</p> <ol style="list-style-type: none"> 1. deny: Reject packets. Applicable to both IPv4 and IPv6.

Parameter	Description
	<p>2. dst-nat: Performs destination NAT on packets. Forward packets from source network to destination; re-mark them with destination IP of the target network. This action functions in tunnel/decrypt-tunnel forwarding mode. User should configure the NAT pool in the managed device.</p> <p>3. src-nat: Performs source NAT on packets. Source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). This action functions in tunnel/decrypt-tunnel/bridge/split-tunnel forwarding mode.</p> <p>4. dual-nat: Performs both source and destination NAT on packets. Source IP and destination IP is changed as per the NAT pool configured. This action functions in tunnel/decrypt-tunnel forwarding mode. User should configure the NAT pool in the managed device.</p> <p>5. permit: Forward packets. Applicable to both IPv4 and IPv6.</p> <p>6. redirect: Specify the location to which packets are redirected. The following are applicable only to IPv4:</p> <ul style="list-style-type: none"> ▪ Datapath destination ID (0-65535). ▪ esi-group: Specify the ESI server group configured with the esi group command. ▪ tunnel: Specify the ID of the tunnel configured with the interface tunnel command. ▪ webcc-reputation: Assign one of the predefined web content reputation levels to the packets. <p>The following are applicable only to IPv6:</p> <ul style="list-style-type: none"> ▪ tunnel: Specify the ID of the tunnel configured with the interface tunnel command. ▪ tunnel-group: Specify the tunnel-group configured with the interface tunnel command. <p>route: Specify the next hop to which packets are routed, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ dst-nat: Destination IP changes to the IP configured from the NAT pool. This action functions in bridge/split-tunnel forwarding mode. User should configure the NAT pool in the managed device. ▪ src-nat: Performs source NAT on packets. Source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). This

Parameter	Description
	action functions in tunnel/decrypt-tunnel/bridge/split-tunnel forwarding mode.
<extended action>	<p>Optional action if rule is applied, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ blacklist/denylist: block user if ACL gets applied. ▪ disable-scanning: pause ARM scanning while traffic is present. Note that you must enable “VoIP Aware Scanning” in the ARM profile for this feature to work. ▪ dot1p-priority: specify 802.1p priority (0-7), where 0 is the lowest priority, and 7 is the highest. ▪ log: generate a log message ▪ mirror: mirror all session packets to datapath or remote destination ▪ If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see firewall on page 636. ▪ next-hop-list: Route packet to the next hop in the list. ▪ position: specify the position of the rule (1 is first, default is last) ▪ queue: assign flow to priority queue (high/low) ▪ send-deny-response: if <action> is deny, send an ICMP notification to the source ▪ time-range: specify time range for this rule (configured with time-range command) ▪ tos: specify ToS value (0-63)
no	Negates any configured parameter.

Example

The following CLI configuration shows how pre-classification and post-classification occurs during enforcement.

Each application has an implicit set of ports that are used for communication. In phase 1, if an application ACE entry is hit, the traffic matching this application’s implicit port is allowed (as governed by the application ACE). The DPI engine can monitor the exchange on these ports and determine the application. Once the application is determined, phase 2 occurs when an evaluation is done to determine the final outcome for the session.

The following CLI configuration example is a user role with both the global and role session ACLs:

```
(host) [mynode] (config) #ip access-list session global-sacl
(host) [mynode] (config) #ip access-list session aprpf-employee-sacl
(host) [mynode] (config) #ip access-list session control
```

```
any any app gmail-chat permit
any any app youtube permit
any any any deny
```

This example shows a DPI rule along with a L3/L4 rule with forwarding action in the same ACL.

```
(host) [mynode] (config) #ip access-list session AppRules
any any app Facebook permit tos 45
any any app YouTube deny
any any appcategory peer-to-peer deny
any any tcp 23 permit
network 40.1.0.0/16 any tcp 80 permit tos 60
network 20.1.0.0/16 any tcp 80 src-nat
!
(host) [mynode] (config) #ip access-list session NetRules
network 80.0.0.0/24 any tcp 80 deny
network 60.0.0.0/24 any tcp 80 dual-nat pool <pool1>
network 10.0.0.0/24 any tcp 80 dst-nat
!
(host) [mynode] (config) #user-role Role1
session-acl AppRules
session-acl NetRules
!
```

The following command configures a session ACL with IPv4 and IPv6 address:

```
(host) [mynode] (config) #ip access-list session common
(host) [mynode] (config-sess-common)#host 10.12.13.14 any any permit
(host) [mynode] (config-sess-common)#ipv6 host 11:12:11:11::2 any any permit
```

The following example displays information for an ACL called mylist:

```
(host) [mynode] (config) #show ip access-list mylist
ip access-list session mylist
mylist
-----
Priority  Source  Destination  Service  Application  Action  TimeRange  Log
Expired  Queue  TOS  8021P  Blacklist/Denylist  Mirror  DisScan  IPv4/6
Contract
-----  -----  -----  -----  -----  -----  -----  ---
-----  -----  -----  -----  -----  -----  -----  -----
```

```
1          any    any          app gmail    deny
Low                                     4
```

The following example shows how this local-override netdestination alias is used in the controller:

```
(host) [mynode] (config) #ip access-list session store-override
```

```

(host) [mynode] (config-sess-store-override)#any alias store any permit
(host) [mynode] (config-sess-store-override)#alias store any any deny
(host) [mynode] (config-sess-store-override)#!
(host) [mynode] (config) #show ip interface brief
Interface                IP Address / IP Netmask      Admin  Protocol
vlan 1                   172.72.10.254 / 255.255.255.0  up     up
vlan 55                  55.55.55.1 / 255.255.255.0    up     up
loopback                 unassigned / unassigned      up     up

(host) [md] #show acl acl-table | include dummy-acl
75  session      620      2          3          dummy-acl
    0

(host) [md] #show acl ace-table acl 75

620: any netdest-id: 34  0  0-0  0-0  f1000080001:permit  alias-dst  hits-
table-index 24578
621: netdest-id: 34 any  0  0-0  0-0  f800080001:permit  alias-src  hits-
table-index 24579
622: any any  0  0-0  0-0  f180000:deny

```

The following examples display the use of extended scope of address range:

```
(host) [mynode] (config) #ip access-list session v6-logon-control
```

```

ipv6 user any udp 546 deny
ipv6 any any svc-v6-icmp permit
ipv6 any any svc-v6-dhcp permit
ipv6 any any svc-dns permit
ipv6 any network fc00::/7 any permit
ipv6 any network fe80::/64 any permit

(host) [mynode] (config) #ip access-list session validuser
network 127.0.0.0 255.0.0.0 any any deny
network 169.254.0.0 255.255.0.0 any any deny
network 224.0.0.0 240.0.0.0 any any deny
host 255.255.255.255 any any deny
network 240.0.0.0 240.0.0.0 any any deny
any any any permit
ipv6 host fe80:: any any deny
ipv6 network fc00::/7 any any permit
ipv6 network fe80::/64 any any permit
ipv6 alias ipv6-reserved-range any any deny
ipv6 any any any permit
!

```

The following example displays the use of source NAT to route the local traffic in AP datapath in Split-Tunnel forwarding mode for IPv6 clients:

```

(host) [mynode] (config) #ip access-list session split
ipv6 any any svc-v6-dhcp permit
ipv6 any any svc-dns permit
ipv6 user network fe80::/16 any permit

```



```
ipv6 network fe::80/16 user any permit
ipv6 user any icmpv6 nb-adv permit
ipv6 user any icmpv6 nb-solicitation permit
ipv6 any user icmpv6 rtr-adv permit
ipv6 any user icmpv6 rtr-solicitation permit
ipv6 any any any route src-nat
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.8.0.0	A new sub-parameter is added to capture a brief description of the session ACL.
ArubaOS 8.4.0.0	The output is modified to display the use of source NAT in Split-Tunnel forwarding mode for IPv6 clients.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip access-list standard

```
ip access-list standard <acname>
  deny {<ipaddr> <wildcard>|any|host <ipaddr>}
  ipv6 <ipaddr>
  no ...
  permit {<ipaddr> <wildcard>|any|host <ipaddr>}
```

Description

This command configures a standard ACL. Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.

Parameter	Description
standard <acname>	Define an access list, where <acname> is an access list name, or an access list number in the specified range. 1-99, 1300-1399
deny	Reject the specified packets, which can be the following: <ul style="list-style-type: none">▪ any: any source▪ host: specify a single host IP address▪ A.B.C.D: IPv4 source address and wildcard
ipv6 <deny permit>	Reject or allow the specified packets, which can be the following: <ul style="list-style-type: none">▪ any: any source/destination IPv6 address▪ host: specify a single host IPv6 address▪ X:X:X:X::X/<1-128>: IPv6 source/destination IPv6 address and wildcard
no	Negates any configured parameter.
permit	Allow the specified packets, which can be the following: IP address and optional wildcard any: any packets host: specify a host IP address

Example

The following command configures a standard ACL:

```
(host) [mynode] (config) #ip access-list standard 1
(host) [mynode] (config-submode) #permit host 10.1.1.244
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

ip cp-redirect-address

```
ip cp-redirect-address {disable | <A.B.C.D>}
```

Description

This command configures a redirect address for captive portal. This command redirects wireless clients that are on different VLANs (from the managed device's IP address) to the captive portal on the managed device.

If you have the Next Generation Policy Enforcement Firewall (PEFNG) license installed in the managed device, modify the captive portal session ACL to permit HTTP/S traffic to the destination **cp-redirect-address <A.B.C.D>** instead of **mswitch**. If you do not have the PEFNG license installed in the managed device, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Parameter	Description
disable	Disables automatic DNS resolution for captive portal.
<A.B.C.D>	Redirect unauthenticated user to this IP address. This address should be routable from all external networks.

Example

The following command configures a captive portal redirect address:

```
(host) ^[mynode] (config) #ip cp-redirect-address disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip default-gateway

```
ip default-gateway
  import {cell|cell-cost <cost>|dhcp|dhcp-cost <cost>|pppoe|pppoe-cost <cost>}
  mgmt <nexthop>
  <nexthop> [<cost>]
```

Description

This command configures the default gateway for Mobility Conductor or the managed device. You can use this command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Conductor or the managed device. If you define more than one dynamic gateway type, you must also define a cost for the route to each gateway. Mobility Conductor or the managed device will first attempt to obtain a gateway IP address using the option with the lowest cost. If Mobility Conductor and the managed device are unable to obtain a gateway IP address, they will then attempt to obtain a gateway IP address using the option with the next-lowest path cost.

Starting from ArubaOS 8.11.0.0, you can use the `ip default-gateway mgmt <nexthop>` command to configure the default gateway on the OOB management port for 7000 Series controllers.

Starting from ArubaOS 8.9.0.0, you can use the `ip default-gateway mgmt <nexthop>` command to configure the default gateway for dedicated OOB management Ethernet port on 7280 controllers.

Parameter	Description
<code>import</code>	Use a gateway IP address obtained through the cell interface, DHCP or PPPoE. The default gateway is imported into the routing table and removed when the uplink is no longer active.
<code>cell</code>	Use a gateway IP address obtained through the cell interface.
<code>cell-cost <cost></code>	Use the cost for cell interface.
<code>dhcp</code>	Use a gateway IP address obtained DHCP.
<code>dhcp-cost <cost></code>	Use the cost for DHCP interface.
<code>pppoe</code>	Use a gateway IP address obtained through PPPoE.
<code>pppoe-cost <cost></code>	Use the cost for PPPoE interface
<code>mgmt <nexthop></code>	Set the default gateway IP address as the management interface IP address.
<code><nexthop> [<cost>]</code>	IP address of the default gateway and the distance metric of this route.

Example

The following command configures the default gateway for the Mobility Conductor:

```
(host) [mynode] (config) #ip default-gateway 10.1.1.1
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The <code>ip default-gateway mgmt <nextHop></code> command can be used to configure the default gateway on the OOB management port for 7000 Series controllers.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp adaptive

ip dhcp adaptive

Description

This command enables adaptive VLAN assignment based on the DHCP server.

Example

The following command enables adaptive VLAN assignment based on the DHCP server:

```
(host) [mynode] (config) #ip dhcp adaptive
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

ip dhcp default-pool

```
ip dhcp default-pool
  private
  public
```

Description

This command configures the DHCP pool type.

Parameter	Description
private	Configure a private DHCP pool.
public	Configure a public DHCP pool.

Example

The following command configures a private DHCP pool:

```
(host) [mynode] (config) #ip dhcp default-pool private
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp excluded-address

```
ip dhcp excluded-address <low-address> [<high-address>]
```

Description

This command configures an excluded address range for the DHCP server on Mobility Conductor. Ensure that the statically assigned IP addresses are excluded.

Parameter	Description
<low-address>	Low range excluded IP addresses. For example, you can enter the IP address of the Mobility Conductor so that this address is not assigned.
<high-address>	High range excluded IP addresses.

Example

The following command configures an excluded address range:

```
(host) [mynode] (config) #ip dhcp excluded-address 192.168.1.1 192.168.1.255
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp increase-lease-limit

ip dhcp increase-lease-limit

Description

This command configures additional DHCP scope that is twice the user limit on specific controller platforms. This feature is disabled by default. This command can be used only in any of the following controller platforms: 7005controller, 7008controller, or 7010controller.

Example

To enable the additional DHCP scope on a controller, execute the following command:

```
(host) (config) #ip dhcp increase-lease-limit
```

Related Commands

Command	Description
show ip dhcp	Shows the DHCP pool statistics.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
7005 controller, 7008 controller, and 7010 controller platforms	Base operating system.	Config mode on the Managed Device or controller.

ip dhcp load-balance

```
ip dhcp load-balance priority
  round-robin {ipupsell | private | public}
  strict {ipupsell | private | public}
```

Description

This command configures the DHCP pool load balancing priority.

Parameter	Description
round-robin	Enable a round-robin priority.
ipupsell	Configure the DHCP pool as an IP upsell pool.
private	Configure the DHCP pool as private.
public	Configure the DHCP pool as public.
strict	Enable a strict priority.
ipupsell	Configure the DHCP pool as an IP upsell pool.
private	Configure the DHCP pool as private.
public	Configure the DHCP pool as public.

Example

The following command DHCP pool load balancing priority:

```
(host) [mynode] (config) #ip dhcp load-balance priority round-robin private
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp option-82

```
ip dhcp option-82 <xml_file_name>
```

Description

This command configures option-82 information through XML file

Parameter	Description
<xml_file_name>	XML file name specifying option-82 information. NOTE: This file must be uploaded to flash before executing this command.

Example

The following example configures reserved entries with MAC address of the device:

```
(host) [mynode] (config) #ip dhcp option-82
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp ping-check

```
ip dhcp ping-check  
disable
```

Description

This command disables the ping-check option on the DHCP server of the Mobility Conductor.

Parameter	Description
disable	Disables the ping-check option on the DHCP server of the Mobility Conductor.

Example

The following example disables the ping-check option on the DHCP server of the Mobility Conductor:

```
(host) [mynode] (config) #ip dhcp ping-check disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp pool

```
ip dhcp pool <name>
  default-router <address> [<address2> <address3> <address4> <address5> <address6>
  <address7> <address8>]
  distributed range <startip> <endip> <hosts>
  dns-server {import | switch-gw-ip | <address> [<address2> <address3> <address4>
  <address5> <address6> <address7> <address8>]}
  domain-name <domain>
  lease <days> <hours> <minutes> <seconds>
  netbios-name-server {import | <address> [<address2> <address3> <address4>
  <address5> <address6> <address7> <address8>]}
  network <network-number> {</prefix(1-30)>|<mask>}
  no ...
  option <code> {hex <hex string> | ip <ipaddr> | text <option-string>}
  pooltype {ipupsell | private | public}
  vendor-class-identifier
```

Description

This command configures a DHCP pool on the Mobility Conductor. A DHCP pool should be created for each IP subnetwork for which DHCP services should be provided. DHCP pools are not specifically tied to VLANs, as the DHCP server exists on every VLAN. When Mobility Conductor receives a DHCP request from a client, it examines the origin of the request to determine if it should respond. If the IP address of the VLAN matches a configured DHCP pool, Mobility Conductor answers the request. When a sub-option, **option 5**, is configured, the DHCP server will allocate an address on the subnet specified in the link-selection sub-option.

Parameter	Description
default-router <address>	IP address of the default router for the DHCP client. The client should be on the same subnetwork as the default router. You can specify up to 8 IP addresses.
distributed range	IP address range for the distributed pool.
<startip>	Starting IP address of the address pool.
<endip>	Ending IP address of the address pool.
<hosts>	Number of clients.
dns-server	Configure DHCP DNS server.
import	Use the DNS server address obtained through DHCP or PPPoE.

Parameter	Description
switch-gw-ip	Configure DNS server as Switch Gateway IP address. Use this parameter when Redirect-DNS has to be enabled on the current pool.
<address>	IP address of the DHCP DNS server. You can specify up to 8 IP addresses.
domain-name <domain>	Domain name to which the client belongs.
lease	The amount of time that the assigned IP address is valid for the client. Specify the lease in <days> <hours> <minutes> <seconds>.
netbios-name-server	IP address of the NetBIOS Windows Internet Naming Service (WINS) server, which can be one of the following:
import	Use the NetBIOS name server address obtained through PPPoE or DHCP.
<address>	IP address of the WINS server. You can specify up to 8 IP addresses.
network	Range of addresses that the DHCP server may assign to clients, in the form of <ipaddr> and <netmask> or <ipaddr> and <prefix>.
</prefix(1-30)>	Network prefix.
<mask>	Network mask.
no	Negates any configured parameter.
option	Client-specific option code and IP address. See RFC 2132, "DHCP Options and BOOTP Vendor Extensions".
hex <hex string>	Specify the Hex string. Maximum hex characters allowed is 22.
ip <ipaddr>	Specify IP address.
text <option-string>	Specify optional string.
pooltype	Configure the DHCP Pool types.
ipupsell	Configure the DHCP pool as an IP upsell pool.
private	Configure the DHCP pool as private.
public	Configure the DHCP pool as public.
vendor-class-identifier	Send or suppress the Aruba AP vendor ID to clients.

Example

The following command configures a DHCP pool:

```
(host) [mynode] (config) #ip dhcp pool floor1
(host) [mynode] (config-submode) #default-router 10.26.1.1
(host) [mynode] (config-submode) #dns-server 192.168.1.10
(host) [mynode] (config-submode) #domain-name floor1.test.com
(host) [mynode] (config-submode) #lease 0 8 0
(host) [mynode] (config-submode) #network 10.26.1.0 255.255.255.0
```

Sub-option Example

The following command configures a sub-option for the DHCP option-82:

```
(host) [mynode] (config) #ip dhcp pool default
(host) [mynode] (config-submode)#option
<code>      DHCP option code(range 0-254)
(host) [mynode] (config-submode)#option 5
(host) [mynode] (config-submode)#option 5
hex       Configure hexadecimal option
ip        Configure IPv4 option
text      Configure text option
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>switch-gw-ip</code> sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip dhcp reserved

```
ip dhcp reserved [hardware-address <mac> ip-address <ipv4> hostname <name>]
```

Description

This command configures DHCP server device reservations. You can use IP reservation to manually bind IP addresses from a DHCP pool to a client MAC address.

Parameter	Description
hardware-address <mac>	The 48-bit MAC address of the device.
ip-address <ipv4>	The fixed IPv4 address of the host.
hostname <name>	Hostname of the managed device.

Example

The following example configures reserved entries with MAC address of the device:

```
(host) [mynode] (config) #ip dhcp reserved hardware-address  
ae:ff:ff:ff:ff:ae ip-address 1.2.3.4 hostname aruba
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip domain-name

ip domain-name <name>

Description

This command configures the default domain name. Mobility Conductor uses the default domain name to complete hostnames that do not contain domain names. You must have at least one domain name server configured on the controller (see [ip name-server on page 869](#)).

Parameter	Description
<name>	Name used to complete unqualified host names. Do not specify the leading dot (.).

Example

The following command configures the default domain name:

```
(host) [mynode] (config) #ip domain-name yourdomain.com
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip domain lookup

ip domain lookup

Description

This command enables DNS hostname to address translation. This command is enabled by default. Use the **no** form of this command to disable.

Example

The following command enables DNS hostname translation:

```
(host) [mynode] (config) #ip domain lookup
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip domain redirect

ip domain redirect

Description

This command enables Domain Name System (DNS) redirect for hostname translation. This command is disabled by default. Use the **no** form of this command to disable.

Example

The following command enables DNS redirect hostname translation:

```
(host) [mynode] (config) #ip domain redirect
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip domain-redirect

```
ip domain-redirect <name> <ip-addr>
```

Description

This command redirects the DNS query matching corporate domain to a dedicated corporate IPv4 DNS server. This command is not enabled by default. Use the **no** form of this command to disable.

Parameter	Description
<name>	Specifies the domain name to be redirected.
<ip-addr>	Specifies the domain server IP address.

Example

The following command redirects the domain to a dedicated DNS server:

```
(host) [mynode] (config) #ip domain-redirect xyzcorp.com 192.168.11.2
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip dynamic-dns

```
ip dynamic-dns interval <interval> server <ipaddr> key <key details> dhcp-pool  
<pool-name>  
ip dynamic-dns push server <ipaddr>
```

Description

This command configures DDNS information.

Parameter	Description
push server	Push DDNS server information. This parameter is available in enable mode only.
<ipaddr>	Specify the IP address of the DDNS server.
interval <interval>	Time interval in seconds at which the DNS updates are synced to the server. 0 to 86400 seconds 43200 seconds
server <ipaddr>	IP address of the server
key <key details>	The key details should be entered in algo-name:keyname:keystring format
dhcp-pool <pool-name>	DHCP pool name

Example

```
(host)[mynode] (config) #ip dynamic-dns interval 3500 server 1.1.1.1 key  
hmac-sha1:ddns-key:asdafsdffasdfsfgdsgs= dhcp-pool pool3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip igmp

```
ip igmp
  last-member-query-count <val>
  last-member-query-interval <last-member-query-interval>
  max-members-per-group <val>
  no
  query-interval <query-interval>
  query-response-interval <query-response-interval>
  quick-client-convergence
  robustness-variable <robustness-variable>
  ssm-range <startip> <maskip>
  startup-query-count <startup-query-count>
  startup-query-interval <startup-query-interval>
  version-1-router-present-timeout <version-1-router-present-timeout>
  version-2-router-present-timeout <version-2-router-present-timeout>
```

Description

This command configures the Internet Group Management Protocol (IGMP) timers and counters. IGMP establishes and manages IP multicast group membership. See RFC 3376, "Internet Group Management Protocol, version 3" for more information.

Parameter	Description
last-member-query-count	Number of group-specific queries that Mobility Conductor sends before assuming that there are no local group members. 1-65535 2
last-member-query-interval	Maximum time, in seconds, that can elapse between group-specific query messages. 1-65535 10
max-members-per-group	Configure maximum members per group. 1-65535 300
query-interval	Interval, in seconds, at which the Mobility Conductor sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information. 1-65535 125

Parameter	Description
query-response-interval	Maximum time, in 1/10th seconds, that can elapse between when the Mobility Conductor sends a host-query message and when it receives a response. This must be less than the query-interval. 1-65535 100
quick-client-convergence	Trigger IGMP reports from client during roaming.
robustness-variable	Increase this value to allow for expected packet loss on a subnetwork. 2-10 2
ssm-range	Configure the start IP address and mask IP address for source-specific multicast range.
startup-query-count	Number of queries that the Mobility Conductor sends out at start up, separated by startup-query-interval . 1-65535 2
startup-query-interval	Interval, in seconds, at which the Mobility Conductor sends general queries on start up. 1-65535 31
version-1-router-present-timeout	Timeout, in seconds, if a version 1 IGMP router is detected. 1-65535 400
version-2-router-present-timeout	Timeout, in seconds, if a version 2 IGMP router is detected. 1-65535 400

Example

The following command configures IGMP:

```
(host) [mynode] (config) #ip igmp
(host) ^[mynode] (config-submode)#query-interval 130
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip local

```
ip local pool <pool_name> <pool_start_address> [<pool_end_address>]
```

Description

This command configures a local IP pool for Layer-2 Tunnel Protocol (L2TP). VPN clients can be assigned IP addresses from the L2TP pool.

Parameter	Description
pool <pool_name>	Name for the address pool.
<pool_start_address>	Starting IP address for the pool.
<pool_end_address>	(Optional) Ending IP address for the pool.

Example

The following command configures an L2TP pool:

```
(host) [mynode] (config) #ip local pool pool-l2tp 10.1.1.1 10.1.1.99
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile active-domain

```
ip mobile active-domain <name>
```

Description

This command configures the mobility domain that is active on Mobility Conductor. All managed devices are initially part of the “default” mobility domain. If you use the “default” mobility domain, you do not need to specify this domain as the active domain on Mobility Conductor. However, once you assign a managed device to a user-defined domain, the “default” mobility domain is no longer an active domain on the Mobility Conductor.

Parameter	Description
<name>	Name of the mobility domain.

Example

The following command assigns Mobility Conductor to a user-defined mobility domain:

```
(host) [mynode] (config) #ip mobile active-domain campus1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile domain

```
ip mobile domain <name>
  anchor <subnet> <netmask> <1-4094> <controller-ip> description <dscr>
  description <descr>
  hat <home-agent> [description <dscr>]
  no
```

Description

This command configures the mobility domain on the managed devices. You configure the HAT on Mobility Conductor; the mobility domain information is pushed to all managed devices that are managed by the same Mobility Conductor.

HAT entries map subnetworks or VLANs and the home agents. The home agent is typically the managed device's IP address. The home agent's IP address must be routable; that is, all managed devices that belong to the same mobility domain must be able to reach the home agent's IP address.

The maximum number of mobility datapath tunnels supported is 32. A maximum of 32 hat entries can be configured if the hat entries are not VRRP IP addresses. If VRRP IP addresses are configured in the HAT table the maximum number of HAT entries supported is less than 32 as for each VRRP entry in HAT more than two datapath tunnels are considered.

The managed device looks up information in the HAT to obtain the IP address of the home agent for a mobile client. Because there can be multiple home agents on a subnetwork, the HAT can contain more than one entry for the same subnetwork.

Parameter	Description
<name>	Name of the mobility domain.
anchor	Configures the anchor managed device. The <code>no ip mobile proxy auth-sta-roam-only</code> command has to be configured for this to work. Supported only for IPv4 clients
<subnet>	VLAN subnet IP of the anchored managed device.
<netmask>	Subnet mask of the anchored managed device.
<1-4094>	VLAN ID of the anchored managed device.
<controller-ip>	The IP address of the anchored managed device.
description	Description of the anchored managed device.
description	Description of the mobility domain. The description can be a maximum of 30 characters (including spaces).

Parameter	Description
hat	Configures a home agent table (HAT) entry.
<home-agent>	The IP address of the home agent managed device that requires mobility service.
description	Description of the HAT entry. The description can be a maximum of 30 characters (including spaces).
no	Negates any configured parameter.

Example

The following command configures HAT entries:

```
(host) [mynode] (config) #ip mobile domain east_building
(host) ^[mynode] (config-submode)#hat 192.0.2.1 description "East building
entries"
(host) ^[mynode] (config-submode)#show ip mobile domain east_building

Mobility Domains:, 1 domain(s)
-----
Domain name east_building

Home Agent Table
Home Agent      Description
-----
192.0.2.1      East building entries
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile foreign-agent

```
ip mobile foreign-agent
  lifetime <40-65534>
  max-visitors <0-5000>
  registrations {interval <100-10000> | retransmits <0-5>}
```

Description

This command configures the foreign agent for IP mobility. A foreign agent is the managed device which handles all mobile IP communication with a home agent on behalf of a roaming client.

Parameter	Description
lifetime	Requested lifetime, in seconds, as per RFC 3344, "IP Mobility Support for IPv4". 40-65534 40
max-visitors	Maximum number of active visitors. 0-5000 5000
registrations	Frequency at which re-registration messages are sent to the home agent:
interval	Retransmission interval, in milliseconds. 100-10000 1000
retransmits	Maximum number of times the foreign agent attempts mobile IP registration message exchanges before giving up. 0-5 3

Example

The following command configures the foreign agent:

```
(host) [mynode] (config) #ip mobile foreign-agent registration interval
10000
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile home-agent

```
ip mobile home-agent
  max-bindings <0-5000>
  replay <0-300>
```

Description

This command configures the home agent for IP mobility. A home agent for a mobile client is the managed device where the client first appears when it joins the mobility domain. The home agent is the single point of contact for the client when it roams.

Parameter	Description
max-bindings	Maximum number of mobile IP bindings. This option is an additional limitation to control the maximum number of roaming users. When the limit is reached, registration requests from the foreign agent fail which causes a mobile client to set a new session on the visited managed device, which will become its home managed device. 0-5000 5000
replay	Time difference, in seconds, for time stamp-based replay protection, as described by RFC 3344, "IP Mobility Support for IPv4". 0 disables replay. 0-300 7

Example

The following command configures the home agent:

```
(host) [mynode] (config) #ip mobile home-agent replay 100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile packet-trace

ip mobile packet-trace <A:B:C:D:E:F>

Description

This command enables packet tracing for the given mac address. This command is used for troubleshooting purposes only.



Use this command with caution. It replaces the existing users with user entries from the imported file.

Platform	License
<A:B:C:D:E:F>	The MAC address of the host

Example

The following command enables packet tracing for the host:

```
(host) [mynode] (config) #ip mobile packet-trace 00:40:96:a6:a1:a4
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile proxy

```
ip mobile proxy
  auth-sta-roam-only
  block-dhcp-release
  event-threshold <1-100>
  log-trail
  no-service-timeout <30-300>
  on-association
  refresh-stale-ip
  stale-timeout <30-3600>
  stand-alone-AP
  trail-length <1-30>
  trail-timeout <120-3600>
```

Description

This command configures the proxy mobile IP module in a mobility-enabled managed device. The *proxy mobile IP module* in a mobility-enabled managed device detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions:

- erives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client.

- etects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP (s) on the same managed device, it is recommended that you keep the **on-association** option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.

Parameter	Description
auth-sta-roam-only	Allows a client to roam only if has been authenticated. If a client has not been authenticated, no mobility service is offered if it roams to a different VLAN or managed device. enabled
block-dhcp-release	Filters out DHCP release from stations.
event-threshold	Maximum number of mobility events (events that can trigger mobility) handled per second. Mobility events above this threshold are ignored. This helps to control frequent mobility state changes when the client bounces back and forth on APs before settling down. 1-100

Parameter	Description
	25
log-trail	Enables logging at the notification level for mobile client moves. enabled
no-service-timeout	Time, in seconds, after which mobility service expires. If nothing has changed from the previous state, the client is given another bridge entry but it will have limited connectivity. 3-300 180
on-association	Enabling this option triggers mobility on station association. Mobility move detection is performed when the client associates with the managed device and not when the client sends packets. Mobility on association can speed up roaming and improve connectivity for devices that can trigger mobility if they do not send many uplink packets. Downside is security; an association is all it takes to trigger mobility. This option is applicable only if layer-2 security is enforced. It is recommended to retain the default settings as this option causes more load in the system due to exchange of extra messages between managed device in the mobility domain. disabled
refresh-stale-ip	Mobility forces station to renew its stale IP (assuming its DHCP) by deauthorizing the station.
stale-timeout	Number of seconds the mobility state is retained after the loss of connectivity. This allows authentication state and mobility information to be preserved on the home agent managed device. The default is 60 seconds but can be safely increased. Note that in many case a station state is deleted without waiting for the stale timeout; user delete from management, foreign agent to foreign agent hand-off, etc. (This is different from the no-service-timeout; no-service-timeout occurs up front while the stale-timeout begins when mobility service is provided but the connection is disrupted for some reason.) 30-3600 60
stand-alone-AP	Enables support for third party or stand-alone APs. When this is enabled, broadcast packets are not used to trigger mobility and packets from untrusted interfaces are accepted. If mobility is enabled, you must also enable stand-alone AP for the client to connect to the managed device's untrusted port. If the managed device learns wired users via the following methods, enable stand-alone AP:

Parameter	Description
	<ul style="list-style-type: none"> Third party AP connected to the managed device through the untrusted port. Clients connected to ENET1 on APs with two ethernet ports. Wired user connected directly to the managed device's untrusted port. <p>disabled</p> <p>NOTE: When IP mobility is enabled, you must also enable the stand-alone AP Support option so that a Multiplexer (MUX) server can perform properly and display all wired users who are connected to a MUX port.</p>
trail-length	<p>Specifies the maximum number of entries (client moves) stored in the user mobility trail.</p> <p>1-30 30</p>
trail-timeout	<p>Specifies the maximum interval, in seconds, an inactive mobility trail is held.</p> <p>120-3600 600</p>

Example

The following command triggers mobility on station association:

```
(host) [mynode] (config) #ip mobile proxy on-association
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip mobile revocation

```
ip mobile revocation
  interval <100-10000>
  retransmits <0-5>
```

Description

This command configures the frequency at which registration revocation messages are sent. A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.

Parameter	Description
<code>interval</code>	Retransmission interval, in milliseconds. 100-10000 1000
<code>retransmits</code>	Maximum number of times the home agent or foreign agent attempts mobile IP registration or revocation message exchanges before giving up. 0-5 3

Example

The following command configures registration revocation messages:

```
(host) [mynode] (config) #ip mobile revocation interval 2000
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip name-server

```
ip name-server <A.B.C.D>
```

Description

This command configures servers for name and address resolution. You can configure up to six servers using separate commands. Specify one or more servers when you configure a default domain name (see [ip domain-name on page 846](#)).

Parameter	Description
<A.B.C.D>	IP address of the server.

Example

The following command configures a name server:

```
(host) [mynode] (config) #ip name-server 10.1.1.245
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip nat

```
ip nat pool <name> <start-ipaddr> <end-ipaddr> [<dest-ipaddr> <static>]
```

Description

This command configures a pool of IP addresses for network address translation (NAT). This command can be referenced to a session ACL rule (see [ip access-list session on page 823](#)).

Parameter	Description
<name>	Name of the NAT pool.
<start-ipaddr>	IP address that defines the beginning of the range of source NAT addresses in the pool.
<end-ipaddr>	IP address that defines the end of the range of source NAT addresses in the pool.
<dest-ipaddr>	Destination NAT IP address.
<static>	Map the NAT pool on a one-to-one basis.

Example

The following command configures a NAT pool:

```
(host) [mynode] (config) #ip nat pool 2net 2.1.1.1 2.1.1.125
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license.	Config mode on Mobility Conductor.

ip nexthop-list

```
ip nexthop-list <STRING>
  ip
    dhcp vlan <id>
      priority <number>
      probe_wan_hc_ip
      <ipaddress>
    ipsec-map <map_name> [priority <number>]
  no
  preemptive-failover
```

Description

Define a next hop list for policy-based routing.

A next hop IP is the IP address of a adjacent router or device with layer-2 connectivity to the managed device. If the managed device uses policy-based routing to forwards packets to a next hop device and that device becomes unreachable, the packets matching the policy will not reach their destination. The next hop list provides redundancy for the next hop devices by forwarding the traffic to a backup next hop device in case of failures. If active next hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next hop on the list.

A maximum of 4 next hops can be added to a next hop list. Each next hop can be assigned a priority, which decides the order of selection of the next hop. If a higher priority next hop goes down, the next higher priority next hop which is active is chosen for forwarding. If all the next hops are configured with same priority, the order is determined based on the order in which they are configured. If all the next hops are down, traffic will not be passed through the regular destination based forwarding.

In a typical deployment scenario with multiple up-links, the default route only uses one of the uplink next-hops for forwarding packets. If a next hop becomes unreachable, the packets will not reach their destination. If your deployment uses policy-based routing based on a next hop list, any of the uplink next hops could be used for forwarding traffic. This requires a valid ARP entry (route-cache) in the system for all the policy-based routing next hops.

In a branch office managed device deployment, the site up-links can obtain their IP addresses and default gateway using DHCP. In such deployments, the next hop-list configuration can use the VLAN IDs of uplink VLANs. If the VLAN gets an IP address using DHCP, and the default gateway is determined by the VLAN interface, the gateway IP is used as the next hop IP address. Branch deployments may also require policy-based redirection of traffic to different VPN tunnels. The next hop list allows you to select an IPsec map to redirect traffic through IPsec tunnels.

Parameter	Description
<STRING>	Name of the next hop list.

Parameter	Description
<code>ip</code>	Next hop IP address.
<code>dhcp vlan <id></code>	VLAN ID of the VLAN used by the next hop device. If the VLAN gets an IP address using DHCP, and the default gateway is determined by the VLAN interface, the gateway IP is used as the next hop IP address.
<code>priority <number></code>	Next hop selection priority.
<code>probe_wan_hc_ip</code>	Enables next hop failover, if the uplink health check of the next hop is unreachable
<code><A.B.D.C></code>	IP address of the next hop device.
<code>ipsec-map <map_name></code>	Packets can be redirected over a VPN tunnel by specifying the IPsec map name.
<code>preemptive-failover</code>	Enable or disable preemptive failover. If preemption is enabled and a higher priority next hop becomes reachable again, packets are again forwarded to the higher priority next hop.

Example

The following command configures a list of next hops:

```
(host) [mynode] (config) #ip nexthop-list list1
(host) ^[mynode] (config-submode)#ip 10.1.1.41 priority 1
(host) ^[mynode] (config-submode)#ip 172.21.18.170 priority 2
(host) ^[mynode] (config-submode)#ip 192.18.140.20 priority 3
```

Related Commands

Command	Description
show ip nexthop-list	Display next hop list settings for policy-based routing.

Command History

Release	Modification
ArubaOS 8.7.1.1	The <code>probe_wan_hc_ip</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip probe data-vpnc

ip probe data-vpnc

Description

This command configures IP probe profile for data VPN concentrator.

Examples

The following commands enable this feature, and reduce the default probe frequency interval and probe burst size.

```
(host) [mynode] (config) #ip probe data-vpnc
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip probe default

```
ip probe default
  burst-size <size>
  frequency <seconds>
  mode ping
  no
  retries <count>
```

Description

This command configures IP probes for the policy-based routing using a next-hop list. The health-check feature uses ping-probes to check reachability and latency from the managed device to data center through each of the managed device's WAN up-links. Latency is calculated based on the round-trip time (RTT) of ping responses. Ping settings are configured globally using the `ip probe default` command.

Parameter	Description
<code>burst-size</code> <size>	Number of probes to be sent during the probe frequency interval defined by the <code>frequency</code> parameter of this profile. 1-16 5
<code>frequency</code> <seconds>	Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the <code>burst-size</code> parameter during each frequency interval defined by this <code>frequency</code> parameter. 10-3600 10
<code>mode ping</code>	Enable this feature by issuing the <code>mode ping</code> command. Ping is the only mode currently supported by this feature.
<code>no</code>	Remove or negate any configured parameter.
<code>retries</code> <count>	Number of times the managed device attempts to resend a probe. 1-255 3

Examples

The following commands enable this feature, and reduce the default probe frequency interval and probe burst size:

```
(host) [mynode] (config) #ip probe default
(host) ^[mynode] (config-submode)#burst-size 3
(host) ^[mynode] (config-submode)#frequency 5
(host) ^[mynode] (config-submode)#mode ping
```

Related Commands

Command	Description
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device up-links.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip probe health-check

```
ip probe health-check
  burst-size <size>
  frequency <frequency>
  mode {ping|udp}
  jitter
  no
  retries <count>
```

Description

This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device up-links. The health-check feature uses ping-probes to check reachability and latency from the managed device to data center through each of the managed device's WAN up-links. Latency is calculated based on the delay of ping responses.

Parameter	Description
<code>burst-size</code> <size>	Number of probes to be sent during the probe frequency interval defined by the <code>frequency</code> parameter of this profile. 1-16 5
<code>frequency</code> <seconds>	Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the <code>burst-size</code> parameter during each frequency interval defined by this <code>frequency</code> parameter. 10-3600 10
<code>jitter</code>	Jitter is a variation in the delay of received packets, which can be worsened by network congestion, improper queuing and configuration errors. The WAN health-check feature measures jitter on the connection to the remote host by sending and measuring packets at fixed intervals. Jitter measurements are only available if the health-check feature is set to send UDP packets.
<code>mode</code> {ping udp}	Enable this feature by issuing the mode command and choosing the type of probe packets to be sent, ping or udp .
<code>no</code>	Remove or negate any configured parameter.
<code>retries</code> <count>	Number of times the managed device attempts to resend a probe. 1-255 3

Examples

The following commands enable this feature, and reduce the default probe frequency interval and probe burst size.

```
(host) [mynode] (config) #ip probe health-check
(host) ^[mynode] (config-submode)#burst-size 3
(host) ^[mynode] (config-submode)#frequency 5
(host) ^[mynode] (config-submode)#mode udp
(host) ^[mynode] (config-submode)#jitter
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip radius

```
ip radius
nas-ip {nas-vlan <nasvlan>|<A.B.C.D>}
rfc-3576-server udp-port <0-65535>
source-interface {loopback|vlan <1-4094>}
```

Description

This command configures global parameters for RADIUS servers. If the `aaa authentication-server radius` command configures a server-specific NAS IP, the server-specific IP address is used instead.

Parameter	Description
<code>nas-ip</code>	A global Network Access Server (NAS) IP address to send in RADIUS packets. This configuration supersedes the server-specific NAS IP configured with the <code>aaa authentication-server radius</code> command.
<code>nas-vlan</code>	Configure the NAS VLAN to be used as the NAS IP address.
<code>A.B.C.D</code>	Configure the NAS IP address.
<code>rfc-3576-server udp-port <0-65535></code>	Configures the UDP port to receive requests from a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, "Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)". See the <code>aaa rfc-3576-server</code> command to configure the server. 0-65535 3799
<code>source-inter face</code>	Interface for all outgoing RADIUS packets. The IP address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:
<code>loopback</code>	Use the IP address of the loopback interface.
<code>vlan</code>	Use the IP address of the VLAN. 1-4094

Example

The following command configures a global NAS IP address sent in RADIUS packets:

```
(host) [mynode] (config) #ip radius nas-ip 192.168.1.245
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	The <code>ip radius rfc-3576-server udp-port</code> command requires the PEFNG license. Other commands are available in the base operating system.	Config mode on Mobility Conductor.

ip route

```
ip route <destip> <destmask> {ipsec <name> [<cost>]|null <0-0>|<nexthop> [<cost>]}
```

Description

This command configures a static route on Mobility Conductor or the managed device. Use the `ip default-gateway` command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Conductor or the managed device.

Parameter	Description
<destip>	Enter the destination IP address prefix in dotted decimal format (A.B.C.D).
<destmask>	Enter the destination netmask in dotted decimal format (A.B.C.D).
ipsec <name>	Enter the IPsec map name to use a static IPsec route map.
null <0-0>	Enter the key word null 0 to designate a null interface.
<nexthop> [<cost>]	Enter the forwarding router address in dotted decimal format (A.B.C.D). Optionally, enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.

Example

The following command configures a static route:

```
(host) [mynode] (config) #ip route 172.16.0.0 255.255.0.0 10.1.1.1
```

Related Commands

Command	Description
ip nexthop-list	Configure next hop list settings for policy-based routing.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base Operating System.	Config mode on Mobility Conductor.

ip tunnel pool

```
ip tunnel pool <pool-name>  
  distributed range <startip> <endip>  
no
```

Description

This command configures the DHCP address pool for remote IP address distribution. This command should be configured from the **/md** node hierarchy.

Parameter	Description
distributed range <startip> <endip>	Configures the DHCP address pool for remote IP address distribution.
no	Remove or negate any configured parameter.

Example

The following command configures the DHCP address pool for remote IP address distribution:

```
(host) [md] (config) #ip tunnel pool corp-tunnel-remote  
(host) ^[md] (config-submode)#distributed range 10.0.0.1 10.0.0.100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip vlan pool

```
ip vlan pool <pool-name>
  distributed range <startip> <endip>
no
```

Description

This command configures the VLAN address pool for remote IP address distribution. This command should be configured from the **/md** node hierarchy.

Parameter	Description
distributed range <startip> <endip>	Configures the VLAN address pool for remote IP address distribution.
no	Remove or negate any configured parameter.

Example

The following command configures the VLAN address pool for remote IP address distribution:

```
(host) [md] (config) #ip VLAN pool corp-vlan-remote
(host) ^[md] (config-submode)#distributed range 10.0.0.1 10.0.0.100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ip-flow-export-profile

```
ip-flow-export-profile
  collector-ip <collector-ip>
  enable
  flow-cache-size <flow-cache-size>
  no
  observation-domain <observation-domain>
  port <port>
  transport-protocol {tcp | udp}
  upload-all-interval <upload-all-interval>
  upload-snapshot-interval <upload-snapshot-interval>
  upload-template-interval <upload-template-interval>
  wireless-export
```

Description

This command configures the IP flow collector profile. This command should be configured under **/md**.

Parameter	Description
collector-ip <collector-ip>	Assigns a managed device as the IP Flow Collector within its node.
enable	Enables the IP Flow Collector.
flow-cache-size <flow-cache-size>	Determines the maximum number of entries a managed device can cache before the log is exported to the IP Flow Collector. 5000–25000
no	Negates the prior configuration.
observation-domain <observation-domain>	Allows the IP Flow Collector to group managed devices when receiving data sessions. Switch IP as 32 Bit number
port <port>	Assigns the port to which the exported caches are sent on the IP Flow Collector.
transport-protocol	Determines the transport protocol when a cache is exported.
tcp	Assigns TCP as the transfer protocol .
udp	Assigns UDP as the transfer protocol.
upload-all-interval <upload-all-interval>	Determines the maximum time interval allowed before a managed device must export its cache to the IP Flow Collector.

Parameter	Description
	0–30 minutes, 0 to disable
upload-snapshot-interval <upload-snapshot-interval>	Determines the maximum time interval cache for an inactive flow is exported. 0–30 minutes, 0 to disable
upload-template-interval <upload-template-interval>	Determines the maximum time interval to upload IPFIX templates. 0–30 minutes, 0 to disable 0
wireless-export	Enables wireless export. Disabled

Example

The following command configures a DHCP pool:

```
(host) [mynode] (config) #ip-flow-export-profile
(host) [mynode] (IP Flow Collector Profile) #enable
(host) [mynode] (IP Flow Collector Profile) #collector-ip 192.0.2.1
(host) [mynode] (IP Flow Collector Profile) #write memory
```

Related Commands

Command	Description
show ip-flow-export wireless-cache	Displays the cache for WLAN information.

Command History

Release	Modification
ArubaOS 8.0.1.0	The <code>wireless-export</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on the Mobility Conductor.

ipv6 cp-redirect-address

ipv6 cp-redirect-address <ip6addr> | disable

Description

This command configures a redirect address for captive portal. This command redirects wireless clients that are on different VLANs (from the managed device's IP address) to the captive portal on the managed device.

If you have the Next Generation PEFNG license installed in the managed device, modify the captive portal session ACL to permit HTTPS traffic to the destination **cp-redirect-address <ip6addr>** instead of **mswitch**. If you do not have the PEFNG license installed in the managed device, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Parameter	Description
<ip6addr>	This address should be routable from all external networks.
disable	Disables automatic DNS resolution for captive portal.

Example

The following command configures a captive portal redirect address:

```
(host) [/md] (config) #ipv6 cp-redirect-address
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 default-gateway

```
ipv6 default-gateway mgmt <ipv6-address> <cost>
```

Description

This command configures an IPv6 default gateway.

Parameter	Description
mgmt	Specify the Management Interface.
<ipv6-address>	Specify the IPv6 address of the default gateway.
cost	Specify the distance metric to select the routing protocol that determines the way to learn the route.

Example

The following command configures an IPv6 default gateway:

```
(host) [/md] (config) #ipv6 default-gateway 2cce:205:160:100::fe 1
```

The following example displays the use of extended scope of address range:

```
(host) [/md] (config) #ipv6 default-gateway 2014::1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 dhcp excluded-address

```
ipv6 dhcp excluded-address <low-address> [<high-address>]
```

Description

This command configures an excluded IPv6 address range for the DHCPv6 server on the Mobility Conductor. Ensure that the statically assigned IPv6 addresses are excluded.

Parameter	Description
<low-ipaddr>	Low end of range of IPv6 addresses. For example, you can enter an IPv6 address that should not be assigned.
<high-ipaddr>	High end of the range of IPv6 addresses.

Example

The following command configures an excluded IPv6 address range:

```
(host) [/md/X.X.X.X.X] (config-dhcpv6)#ipv6 dhcp excluded-address  
2002:570:20::2 2002:570:20::25
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in base operating system.	Config mode on Mobility Conductor.

ipv6 dhcp pool

```
ipv6 dhcp pool <pool-name>
  dns-server {switch-gw-ipv6 | <ipv6-address>}
  domain-name <domain>
  lease <days> <hours> <minutes> <seconds>
  network <network prefix>
  no ...
  option <code> {ip <ipv6-addr> | text <string>}
  preference <1-255>
```

Description

This command configures a DHCPv6 pool on the Mobility Conductor. A DHCPv6 pool should be created for each IPv6 subnetwork for which DHCPv6 services should be provided. DHCPv6 pools are not specifically tied to VLANs, as the DHCPv6 server exists on every VLAN. When the Mobility Conductor receives a DHCPv6 request from a client, it examines the origin of the request to determine if it should respond. If the IPv6 address of the VLAN matches a configured DHCPv6 pool, the Mobility Conductor answers the request.

Parameter	Description
dns-server	IPv6 address of the DNS server.
switch-gw-ipv6	Configure DNS server as Switch Gateway IPv6 address. Use this parameter when Redirect-DNS has to be enabled on the current pool.
<ipv6-address>	IPv6 address of the DHCP DNS server.
domain-name	Domain name to which the client belongs.
lease	The amount of time that the assigned IPv6 address is valid for the client. Specify the lease in <days> <hours> <minutes> <seconds>. The default value is 12 hours.
network	The DHCPv6 network prefix.
no	Negates any configured parameter.
option	Client-specific option code and IPv6 address or text. See RFC 3315, DHCPv6.
preference	The DHCPv6 server preference.

Example

The following command configures a DHCPv6 pool:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 dhcp pool DHCPv6
(host) [/md/X.X.X.X.X.X] (config-submode) #dns-server 2001:470:20::2
(host) [/md/X.X.X.X.X.X] (config-submode) #domain-name test.org
(host) [/md/X.X.X.X.X.X] (config-submode) #lease 0 12 0 0
(host) [/md/X.X.X.X.X.X] (config-submode) #network 2001:470:20::/64
(host) [/md/X.X.X.X.X.X] (config-submode) #option 24 text "Domain Search
List"
(host) [/md/X.X.X.X.X.X] (config-submode) #preference 25
```

The following example displays the use of extended scope of address range, which is restricted only to DHCP pool configuration:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 dhcp pool sparta
network 2012::/120
!
```



If the DHCP pool configuration on the managed device, that acts as a DHCP server has the address pool configured in the reserved range, then the APs get an IP address from the server. If the address pool is not in the reserved range, then the AP cannot get an IP from the server.

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>switch-gw-ipv6</code> sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 dhcp relay-option

```
ipv6 dhcp relay-option <xml_file_name>
```

Description

This command configures the DHCPv6 relay options by using XML file. The XML definition file allows you to configure DHCPv6 Option 18 (Circuit ID) and Option 37 (Remote ID) sub-type options.



You must upload the XML file to Mobility Conductor flash file system, before issuing this command.

Example

The following example configures a DHCPv6 Relay-Option:

```
(host)[mynode](config) #ipv6 dhcp relay-option my_dhcp_relay-option.xml
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 domain lookup

ipv6 domain lookup

Description

This command enables IPv6 Domain Name System hostname translation for clients.

Example

The following command enables IPv6 Domain Name System hostname translation:

```
(host) [mynode] (config) #ipv6 domain lookup
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>lookup</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 domain-redirect

```
ipv6 domain-redirect <name> <ipv6-addr>
```

Description

This command redirects the domain to a dedicated DNS server in the IPv6 domain. This command is enabled by default. Use the **no** form of this command to disable.

Parameter	Description
<name>	Specifies the domain name to be redirected.
<ipv6-addr>	Specifies the domain server IPv6 address.

Example

The following command redirects the domain to a dedicated DNS server:

```
(host) [mynode] (config) #ipv6 domain-redirect xyzcorp.com 2001:0000::1101
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 enable

ipv6 enable

Description

This command enables IPv6 packet processing globally. This option is disabled by default.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 firewall

```
ipv6 firewall
  attack-rate {ping <number>|session <number>|tcp-syn <number>}
  deny-inter-user-bridging |
  drop-ip-fragments |
  enable-per-packet-logging |
  enable-stateful-icmp |
  enforce-tcp-handshake |
  enforce-tcp-sequence |
  ext-hdr-parse-len |
  no
  prohibit-ip-spoofing |
  prohibit-rst-replay |
  session-idle-timeout <seconds>
```

Description

This command configures firewall options on the Mobility Conductor for IPv6 traffic.

Parameter	Description
attack-rate	Sets rates which, if exceeded, can indicate a denial of service attack.
ping	Number of ICMP pings per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 120. 1-16384
session	Number of TCP or UDP connection requests per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 960. 1-16384
tcp-syn	Number of TCP SYN messages per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 960. 1-16384
deny-inter-user-bridging	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent Appletalk or IPX traffic from being forwarded. disabled
drop-ip-fragments	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by a customer support representative.

Parameter	Description
	disabled
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by a customer support representative, as doing so may create unnecessary overhead on the Mobility Conductor. disabled
enforce-stateful-icmp	Enables stateful ICMP processing and create sessions for ICMP errors and denies unidirectional response. disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network. disabled
enforce-tcp-sequence	Prevents data from passing between two clients until the three-way TCP sequence numbers are exchanged.
ext-hdr-parse-len	Set the threshold value beyond which the IPv6 header will not be parsed and the packet will be dropped. 100 bytes
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent. disabled
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by a customer support representative. disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by a customer support representative. 16-300 16 seconds

Example

The following command does not allow forwarding of non-IP frames between IPv6 clients:

```
(host) [/md] (config) #ipv6 firewall deny-inter-user-bridging
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system, except for noted parameters.	Config mode on Mobility Conductor.

ipv6 helper-address

```
ipv6 helper-address  
  helper-address <address>  
  source <srcaddr>
```

Description

This command configures the DHCPv6 server relay agent. .

Parameter	Description
helper-address	Configures DHCPv6 server relay agent.
source	Configure DHCPv6 relay source address if the interface has more than one IPv6 address.

Example

The following command configures a helper address:

```
(host) [00:0c:29:3c:f7:d3] (config-submode)#ipv6 helper-address 2017::2  
source 2016::2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 kernel-disable

```
ipv6 kernel-disable  
no...
```

Description

This command disables IPv6 configurations in the Linux Kernel systems.

Example

The following command disables IPv6 configurations in the Linux Kernel systems

```
(host) [mynode] (config) #ipv6 kernel-disable
Please ensure all IPv6 configurations are removed including global IPv6
config knob. This config will reboot the controller. Do you want to continue
(y/n) ?:
```

Command History

Release	Modification
ArubaOS 8.6.0.10	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 local

```
ipv6 local  
  pool <pool_name_v6> <pool_start_addressv6> <pool_end_addressv6>
```

Description

This command configures a local IPv6 pool for Layer-2 Tunnel Protocol (L2TP). VPN clients can be assigned IPv6 addresses from the L2TP pool.

Parameter	Description
pool	Name for the address pool.
<pool_start_addressv6>	Starting IPv6 address for the pool.
<pool_end_addressv6>	(Optional) Ending IPv6 address for the pool.

Example

The following command configures a local IPv6 pool:

```
(host) [mynode] (config) #ipv6 local pool  
2001:0000:0eab:DEAD:0000:00AO:ABCD:004E  
2002:0000:0eab:DEAD:0000:00AO:ABCD:004E
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 name-server

```
ipv6 name-server  
X:X:X:X::X
```

Description

This command configures the IPv6 address of the domain name server.

Parameter	Description
X:X:X:X::X	Domain server IPv6 address (maximum of 6).

Example

The following command adds IPv6 name server (DNS server):

```
(host) [mynode] (config) #ipv6 name-server 2020::abcd:abcd
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The domain server IPv6 address was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 neighbor

ipv6 neighbor <ipv6addr> vlan <vlan#> <mac>

Description

This command configures an IPv6 static neighbor on a VLAN interface.

Parameter	Description
<ipv6addr>	Specify the IPv6 address of the neighbor entry.
vlan <vlan#>	Specify the VLAN ID.
<mac>	Specify the 48-bit hardware address of the neighbor entry.

Example

The following command configures an IPv6 static neighbor on VLAN 1:

```
(host) [/md/X.X.X.X.X] (config) #ipv6 neighbor 2cce:205:160:100::fe vlan 1  
00:0b:86:61:13:28
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 nexthop-list

```
ipv6 nexthop-list <STRING>
  ipsec6-map <map_name> [priority <number>]
  ipv6 {<X:X:X:X:X:X:X> [priority <number>]}
  no
  preemptive-failover
```

Description

This command defines a next-hop list for IPv6 address in policy-based routing.

A next-hop IP is the IPv6 address of an adjacent router or device with layer-2 connectivity to the managed device. If the managed device uses policy-based routing to forwards packets to a next-hop device and that device becomes unreachable, the packets matching the policy will not reach their destination. The next-hop list provides redundancy for the next-hop devices by forwarding the traffic to a backup next-hop device in case of failures. If active next-hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next-hop on the list. You can verify the reachability by using `show ip health-check` command. All the next-hop IPv6 addresses are added to the health-check if the next-hop is used by a route ACL. The datapath uses only the next-hop devices that are reachable.

A maximum of 16 next-hops can be added to a next-hop list. Each next-hop can be assigned a priority, which decides the order of selection of the next-hop. If a higher priority next-hop goes down, the next higher priority next-hop which is active is chosen for forwarding. If all the next-hops are configured with same priority, a round-robin order is used. If all the next-hops are down, traffic is dropped and regular destination based forwarding happens when IPv6 forward rule is configured explicitly in ACL for PBR.

In a typical deployment scenario with multiple up-links, the default route only uses one of the uplink next-hops for forwarding packets. If a next-hop becomes unreachable, the packets will not reach their destination. If your deployment uses policy-based routing based on a next-hop list, any of the uplink next-hops could be used for forwarding traffic. This requires a valid ARP entry (route-cache) in the system for all the policy-based routing next-hops.

Branch deployments may also require policy-based redirection of traffic to different site-to-site tunnels. The next-hop list allows you to select an IPsec map to redirect traffic through IPsec tunnels.



A maximum of 32 next-hop lists (IPv4 and IPv6) is allowed.

Parameter	Description
<STRING>	Name of the next-hop list. NOTE: You cannot use the same name for both IPv4 and IPv6 next-hop lists.

Parameter	Description
<code>ipsec6-map <map_name></code>	Packets can be redirected over a site-to-site tunnel by specifying the IPsec map name. NOTE: Only site-to-site VPN is currently supported for IPv6. Hence, the IPsec map is limited to the site-to-site map.
<code>[priority <number>]</code>	(Optional) Use this parameter to assign priority to next-hop. 1-255 128
<code>ipv6 <X:X:X:X:X:X:X></code>	IPv6 address of the next-hop device.
<code>[priority <number>]</code>	(Optional) Use this parameter to assign priority to next-hop. 1-255 128
<code>no</code>	Negates any configured parameter.
<code>preemptive-failover</code>	Enable or disable preemptive failover. If preemption is enabled and a higher priority next-hop becomes reachable again, packets are again forwarded to the higher priority next-hop. NOTE: This option is enabled by default.

Example

The following command configures a list of next-hops:

```
(host) [mynode] (config) #ipv6 nexthop-list new
(host) ^[mynode] (config-submode)#ipv6 2005::1 priority 1
(host) ^[mynode] (config-submode)#ipv6 2002::2 priority 2
(host) ^[mynode] (config-submode)#ipv6 2008::4 priority 3
```

Related Commands

Command	Description
show ipv6 nexthop-list	Display IPv6 next-hop list settings for policy-based routing.
show ip health-check	Display the health-check status of the uplink interfaces of a branch office managed device.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 mld

```
ipv6 mld
  max-members-per-group <val>
  no
  query-interval <query-interval>
  query-response-interval <query-response-interval>
  robustness-variable <robustness-variable>
  ssm-range <startip> <maskip>
```

Description

This command configures the IPv6 MLD (Multi-listener discovery) parameters. You can modify the default values of the MLD parameters for IPv6 MLD snooping. You must enable IPv6 MLD snooping for these values to take effect. For more information on enabling IPv6 MLD snooping, see [interface vlan on page 776](#).

Parameter	Description
max-members-per-group	Configure maximum members per group (1-65535). The default value is 300.
query-interval	Specify the time interval in seconds (1-65535) between general queries. The default value is 125 seconds. By varying this value, you can tune the number of MLD messages on the link; larger values cause MLD queries to be sent less often.
query-response-interval	Specify the maximum response delay in deciseconds (1/10 seconds) that can be inserted into the periodic general queries. The default value is 100 deciseconds. By varying this value, you can tune the burstiness of MLD messages on the link; larger values make the traffic less bursty, as node responses are spread out over a larger interval. The number of seconds represented by this value must be less than the query interval.
robustness-variable	Specify a value between 2 to 10. The default value is 2. The robustness variable allows you to tune for the expected packet loss on a link. If a link is expected to be lossy, you can increase this value. You must not configure the robustness variable as 0 or 1.
ssm-range	Specify the source specific multicast IPv6 range. This variable allows you to configure a valid multicast IPv6 address range for which SSM semantics needs to be applied. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF.

Example

The following command configures the query interval of 200 seconds for IPv6 MLD snooping:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 mld
(host) [/md/X.X.X.X.X.X] (config-mln) # query-interval 200
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>max-members-per-group</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on managed devices.

ipv6 proxy-ra

```
ipv6 proxy-ra  
  interval <value>
```

Description

This command configures an interval for proxy RA.

Parameter	Description
interval	Configures the proxy RA interval (180-1800 sec). This overrides interface RA interval value if it is lesser.

Example

The following command enables proxy RA:

```
(host) [md] (config) #ipv6 proxy-ra  
IPv6 RA proxy already enabled.
```

The following command configures a global NAS IPv6 address sent in RADIUS packets:

```
(host) [md] (config) #ipv6 proxy-ra interval 200
```

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>proxy-ra</code> parameter was modified to enable proxy RA.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 radius

```
ipv6 radius
  nas-ip6 { nas-vlan <nasvlan>|<ipv6-addr>}
  source-interface {loopback|vlan <vlan> <ip6addr>}
```

Description

This command configures global parameters for configured IPv6 RADIUS servers. If the `aaa authentication-server radius` command configures a server-specific NAS IPv6 address, the server-specific IPv6 address is used instead.

Parameter	Description
<code>nas-ip6</code>	A global NAS IPv6 address to send in RADIUS packets. This configuration supercedes the server-specific NAS IPv6 configured with the <code>aaa authentication-server radius</code> command.
<code>nas-vlan <nasvlan></code>	The NAS VLAN to be used as NAS IP.
<code>ipv6-addr</code>	The NAS IPv6 address.
<code>source-interface</code>	Interface for all outgoing RADIUS packets. The IPv6 address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:
<code>loopback</code>	The loopback interface.
<code>vlan</code>	The specified VLAN.

Example

The following command configures a global NAS IPv6 address sent in RADIUS packets:

```
(host) [md] (config) #ipv6 radius nas-ip6 2001:470:20::2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 route

```
ipv6 route {X:X:X:X::X/<0-128>}|ipv6-next-hop|null|vlan[vlanid]|link-local-next-hop}|cost
```

Description

This command configures static IPv6 routes on the managed device.

Parameter	Description
X:X:X:X::X/<0-128>	Specify the IPv6 address and the prefix length of the destination.
<ipv6-next-hop>	Specify the next-hop IPv6 address or null 0 to terminate or discard the packets. Listed below are the following options: <ul style="list-style-type: none">▪ X:X:X:X::X-IPv6 address of next-hop. The address should only be a Global IPv6 address.▪ null-Null interface▪ vlan-Vlan for link local for next-hop▪ <vlanid>-Vlan-id for link local next-hop▪ X:X:X:X::X-IPv6 link local address of next-hop
<cost>	Specify the distance metric to select the routing protocol that determines the way to learn the route.

Example

The following command configures a static IPv6 route on the managed device:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2cce:205:160:100::/<64>
2001:205:160:100::ff 1
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2000:eab::/64 vlan 1
fe80::1a:1e00:a00:9f0
The following example displays the use of extended scope of address range:
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2002::/64 2004::2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

ipv6 tacacs

```
source-interface {loopback|vlan <1-4094> [<ip6addr>]}
```

Description

This command configures parameters for configured IPv6 TACACS servers.

Parameter	Description
source-interface	Select source address of outgoing TACACS requests to the server.
loopback	Use the IPv6 address of the loopback interface.
vlan <1-4094>	Select VLAN of outgoing TACACS requests to the server. 1-4094

Example

The following command configures a VLAN IPv6 address sent in TACACS packets:

```
(host) [mynode] (config) # ipv6 tacacs source-interface vlan 25 192.168.2.55
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ip-reputation deny

ip-reputation deny [inbound|outbound]

Description

This command denies connections matching malicious IP addresses.

Parameter	Description
inbound	Denies connections originated from outside.
outbound	Denies connections originated by managed device.

Example

The following command denies connections originated from outside:

```
(host) [mynode] (config) #ip-reputation deny inbound
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

kernel coredump

[no] kernel coredump



Use this command under the supervision of Aruba Global Technical Support.

Description

This command enables the controller to capture the snapshot of the working memory of the control plane when the control plane has terminated abnormally. An additional flash memory available check is imposed on core dump. If less than 100 MB of space is left on the flash, the extra core dump chunks get discarded. After issuing this command, you may run the `write memory` command to save the configuration. This will enable the kernel core dumps across reboots.

Parameter	Description
coredump	Enable kernel core dump on the controller. Disabled

Example

The following example enables kernel core dump on the controller:

```
(host) (config) #kernel coredump
```

Use the following command to save the configuration change using the CLI:

```
(host) (config) #write memory
```

Use the following command to view the kernel core dump status using the CLI:

```
(host) (config) #show running-config | include kernel
Building Configuration...
kernel coredump
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

kernel printk

kernel printk

Description

This command enables the kernel printk.

Parameter	Description
printk	Enable kernel printk.

Example

The following example enables kernel core dump on the controller:

```
(host) (config) #kernel printk
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lb-group

```
<name>  
  gre-standby  
  hold-time <number>  
  no {gre-standby|hold-time|preemption|primary|randomize-time|secondary}  
  preemption  
  primary  
  randomize-time <number>  
  secondary
```

Description

This command allows you to manage and configure the load balancing group.

Parameter	Description
name	Name of load balancing group
gre-standby	Enable GRE standby
hold-time <number>	Hold time after which failover occurs
no	Disable load balancing group features
preemption	Enable preemptive failover
primary	Configure primary map
randomize-time <number>	Random time after hold-time when failover occurs
secondary	Configure secondary map

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed device.

lc-cluster group-profile



The `active-client-rebalance-threshold`, `standby-client-rebalance-threshold`, and `unbalance-threshold` parameters are not supported from ArubaOS 8.11.0.0 or later versions.

```
lc-cluster group-profile <profile>
  active-ap-lb
  active-ap-rebalance-ap-count <active-ap-rebalance-ap-count>
  active-ap-rebalance-threshold-percentage <active-ap-rebalance-threshold-
percentage>
  active-ap-rebalance-timer <active-ap-rebalance-timer>
  active-ap-unbalance-threshold-percentage <active-ap-unbalance-threshold-
percentage>
  active-client-rebalance-threshold
  clone <source>
  controller <ip> [priority <prio>] [mcast-vlan <mcast_vlan>] [vrrp-ip <vrrp_ip>
vrrp-vlan <vrrp_vlan> group <group number>]
  controller-v6 <ipv6>
  heartbeat-threshold <heartbeat-threshold>
  redundancy
  rapcluster
  standby-client-rebalance-threshold <standby-client-rebalance-threshold>
  unbalance-threshold <unbalance-threshold>
  vrrp-id <starting id>
```

Description

This command is used to configure the cluster group profile in the Mobility Conductor.

Parameter	Description
<profile>	Enter the cluster profile name you want to create.
active-ap-lb	Enable load balancing of APs by load sharing active AACs among cluster members.

Parameter	Description
active-ap-rebalance-ap-count <active-ap-rebalance-ap-count>	Specify the number of APs when active AP rebalance is initiated.
active-ap-rebalance-threshold-percentage <active-ap-rebalance-threshold-percentage>	Redistribute active AP load when active load on any cluster is beyond this configured percentage.
active-ap-rebalance-timer <active-ap-rebalance-timer>	Time, in minutes, to initiate the active AP rebalancing operation.
active-ap-unbalance-threshold-percentage <active-ap-unbalance-threshold-percentage>	Redistribute active AP load when the controller reaches the rebalance threshold and the difference between the maximum and minimum load on the controller is more than this threshold percentage.
active-client-rebalance-threshold	<p>Redistribute active client load when active load on any cluster node is beyond this configured percentage.</p> <p>NOTE: This parameter is not supported</p>

Parameter	Description
	from ArubaOS 8.11.0.0 or later versions.
clone <source>	Copy data from another controller cluster profile.
controller <ip>	Managed device to be made part of this cluster. The IPv4 Address is the value of the controller-ip
priority <prio>	Defines the priority level for the managed devices
mcast-vlan <mcast_vlan>	Enter the multicast vlan
vrrp-ip <vrrp_ip>	Configure the VIP address that will be owned by the elected VRRP master.
vrrp-vlan <vrrp_vlan>	Specifies the VLAN ID of the VLAN on which VRRP will run.
group <group_id>	The value of the parameter is an integer and the range is 1-12. The value 0 is the unset value if you do not want to group the managed devices.

Parameter	Description
<pre>controller-v6 <ipv6></pre>	<p>controller to be made part of this cluster. The IPv6 address is the value of the controller-ip.</p>
<pre>group <group_id></pre>	<p>The value of the parameter is an integer and the range is 1-12. The value 0 is the unset value if you do not want to group the managed devices.</p>
<pre>mcast-vlan <mcast_vlan></pre>	<p>Enter the multicast VLAN to be used for forwarding multicast traffic to upstream router.</p>
<pre>priority <prio></pre>	<p>Define the priority level for the managed devices. The value of this parameter is in the range of 1-255. The default value is 128.</p>
<pre>vrrp-ip-v6 <vrrp_ip_v6></pre>	<p>Configure the IPv6 address that is owned by the elected VRRP master.</p>

Parameter	Description
heartbeat-threshold	Heartbeat threshold is the time in ms that the cluster will wait before declaring a peer cluster node as dead. By default, the value is 900 ms.
redundancy	Enable load sharing redundancy among cluster members.
rapcluster	Enables the cluster behind NAT for Remote APs.
standby-client-rebalance-threshold	<p>Redistribute standby client load when total load on any cluster node is beyond this configured percentage.</p> <p>NOTE: This parameter is not supported from ArubaOS 8.11.0.0 or later versions.</p>
unbalance-threshold	Indicates the minimum difference in load percentage between max loaded cluster node and min loaded cluster node to let load balancing algorithm kick in.

Parameter	Description
	<p>NOTE: This parameter is not supported from ArubaOS 8.11.0.0 or later versions.</p>
<pre>vrrp-id <starting id></pre>	<p>This is an optional parameter which specifies the starting VRRP ID for cluster members. If this is not configured, system automatically configures VRRP groups within the range of 220-225.</p>
<pre>vrrp-passphrase <vrrp passphrase string></pre>	<p>This is an optional password of up to 8 characters that can authenticate VRRP peers in their advertisements. If this is not configured, there is no authentication password.</p>

Example

The following command adds the managed devices to a group profile:

```
(host) [md] (config)lc-cluster group-profile cluster6
(host) [md] (Classic Controller Cluster Profile "cluster6") controller
192.168.28.22 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1
(host) [md] (Classic Controller Cluster Profile "cluster6") controller
192.168.28.23 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1
```



```
(host) [md] (Classic Controller Cluster Profile "cluster6") controller
192.168.28.24 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 2
(host) [md] (Classic Controller Cluster Profile "cluster6") controller
192.168.28.26 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 2
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The following parameters were removed: <ul style="list-style-type: none"> ■ active-client-rebalance-threshold ■ standby-client-rebalance-threshold <standby-client-rebalance-threshold> ■ unbalance-threshold <unbalance-threshold>
ArubaOS 8.7.0.0	The default value of the heartbeat-threshold parameter was changed to 900 ms.
ArubaOS 8.5.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ vrrp-id <starting id> ■ vrrp-passphrase <vrrp passphrase string>
ArubaOS 8.4.0.0	The rapcluster parameter was added.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ active-ap-lb ■ active-ap-rebalance-ap-count ■ active-ap-rebalance-threshold-percentage ■ active-ap-rebalance-timer ■ active-ap-unbalance-threshold-percentage ■ controller-v6 ■ redundancy
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on Mobility Conductor.

lc-cluster group-membership

lc-cluster group-membership

Description

Configure the group-membership in each node. This command is used to enable the cluster membership on the managed devices.

Parameter	Description
<profile>	Enter the cluster profile name.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on managed devices.

lc-cluster start-vlan-probe

lc-cluster start-vlan-probe

Description

This command is used to trigger a VLAN probe on the managed devices. Execute this command to re-run the VLAN probing algorithm after removing the VLANs using the command, `lc-cluster exclude-vlan`.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

lc-cluster exclude-vlan

```
lc-cluster exclude-vlan <excludevlan>
```

Description

This command is used to exclude certain VLANs for the VLAN probing algorithm on the managed devices.

Parameter	Description
<excludevlan>	List of exception VLANs separated by comma (,), range by (-). Max string length: 256.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on managed devices.

Ic-cluster initiate initiate Upgrade

```
lc-cluster initiate initiate
  upgrade
    version <img_version>
      fileserver
      max-downloads
      partition <partition_id>
```

Description

This command is used to trigger the cluster upgrade in the Mobility Conductor:

Parameter	Description
upgrade	Upgrade using information in configured upgrade-profile
version <version_string>	Target image version, for example, 8.1.0.0_XXXXX
fileserver {ftp http scp tftp}	Specify file server details.
max-downloads <ap_preload_batch_size>	Maximum number of simultaneous APs doing image preload. The default is 100 per AAC.
partition <partition_id>	The partition on the managed device to which the new image is to be copied, valid values are 0 or 1 and this is optional. If the partition is not specified, it will automatically pick the alternate boot partition.

Example

```
(host) [mm] [cluster1] #lc-cluster <cluster_name> initiate upgrade version
<img_version> partition <partition_id>
```

cluster_name: The configured cluster profile name, the managed devices and APs associated to the cluster that needs to be upgraded.

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on Mobility Conductor.

Ic-cluster initiate schedule upgrade

```
lc-cluster initiate schedule upgrade
  version <version_string>
    <year> <month> <day> <hh> <mm> <ss>
    max-downloads <ap_preload_batch_size>
    partition <partition_id>
```

Description

This command is used to schedule a cluster upgrade.

Parameter	Description
version	The version to which the cluster will get upgraded to.
year	Year of the upgrade
month	Month of the upgrade
day	Day of the upgrade
hh	Hour of the upgrade
mm	Minutes of the upgrade
ss	Seconds of the upgrade
max-downloads <ap_preload_batch_size>	Maximum number of simultaneous APs doing image preload. The default is 100 per AAC.
partition <partition_id>	The partition on the managed device to which the new image is to be copied, valid values are 0 or 1 and this is optional. If the partition is not specified, it will automatically pick the alternate boot partition.

Example

The following command schedules a cluster upgrade:

```
(host) [mm] (config) #lc-cluster v4 schedule upgrade version 8.4.0.0-
sangiovese_73823 2018 04 10 00 00 00
```

Related Commands

Command	Description
<u>lc-cluster initiate abort</u>	This command is used to delete or abort a scheduled cluster upgrade.
<u>lc-cluster initiate re-schedule upgrade</u>	This command is used to reschedule a scheduled cluster upgrade.
<u>show lc-cluster</u>	Displays information related to vlan, membership, profile, heartbeat, status of the scheduled upgrades and so on for a cluster.
<u>upgrade managed-devices</u>	This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on Mobility Conductor.

Ic-cluster initiate re-schedule upgrade

```
lc-cluster initiate re-schedule upgrade
  version <version_string>
    <year> <month> <day> <hh> <mm> <ss>
    max-downloads
    partition <partition_id>
```

Description

This command is used to reschedule a scheduled cluster upgrade.



To reschedule a cluster upgrade, the upgrade must already be scheduled.

Parameter	Description
version <version_string>	The version to which the cluster will get upgraded to
year	Year of the upgrade
month	Month of the upgrade
day	Day of the upgrade
hh	Hour of the upgrade
mm	Minutes of the upgrade
ss	Seconds of the upgrade
max-downloads <ap_preload_batch_size>	Maximum number of simultaneous APs doing image preload. The default is 100 per AAC.
partition <partition_id>	The partition on the managed device to which the new image is to be copied, valid values are 0 or 1 and this is optional. If the partition is not specified, it will automatically pick the alternate boot partition.

Related Commands

Command	Description
upgrade managed-devices	This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.
lc-cluster initiate abort	This command is used to delete or abort a scheduled cluster upgrade.
lc-cluster initiate schedule upgrade	This command is used to schedule a cluster upgrade.
show lc-cluster	Displays information related to vlan, membership, profile, heartbeat, status of the scheduled upgrades and so on for a cluster.

Example

The following command reschedules a cluster upgrade:

```
(host) [mm] (config)#lc-cluster v4 re-schedule upgrade version 8.2.0.1 2018
6 6 0 50 0
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on Mobility Conductor.

lc-cluster initiate abort

```
lc-cluster initiate abort
  scheduled-upgrade
  upgrade
```

Description

This command is used to delete or abort a scheduled cluster upgrade.

Parameter	Description
scheduled-upgrade	Specify the scheduled cluster upgrade which is to be aborted.
upgrade	Abort the ongoing cluster upgrade.

Related Commands

Command	Description
upgrade managed-devices	This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.
lc-cluster initiate re-schedule upgrade	This command is used to reschedule a scheduled cluster upgrade.
lc-cluster initiate schedule upgrade	This command is used to schedule a cluster upgrade.
show lc-cluster	Displays information related to vlan, membership, profile, heartbeat, status of the scheduled upgrades and so on for a cluster.

Example

The following command deletes or aborts a scheduled cluster upgrade:

```
(host) [mm] (config) #lc-cluster <cluster4node> abort scheduled-upgrade
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system.	Config mode on Mobility Conductor.

lacp group

```
lacp group <group_number> mode {active | passive}
```

Description

This command allows you to enable LACP and configure LACP on the interface. LACP is disabled by default and if the group number assigned contains static port members, the command is rejected.

Parameter	Description
<group_number>	Enter the LAG number. Range: 0-7
mode {active passive}	Enter the keyword mode followed by either the keyword active or passive . <ul style="list-style-type: none">Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets.Passive mode—the interface is <i>not</i> in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.

Related Command

Command	Description
show lacp	View the LACP configuration status.
show interface port-channel	View information on a specified port channel interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lacp port-priority

lacp port-priority <priority_value>

Description

Configure the LACP port priority and set the port priority for LACP.

Parameter	Description
<priority value>	Enter the port-priority value. The higher the value number the lower the priority. 1 to 65535 255

Related Commands

Command	Description
lacp group	Enable LACP and configure on the interface.
show lacp	View the LACP configuration status.
show interface port-channel	View information on a specified port channel interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All Platforms	Base operating system.	Configuration Interface Mode (config-if) for Mobility Conductor.

lacp system-priority

lacp system-priority <priority_value>

Description

This command configures the LACP system priority.

Parameter	Description
<priority_value>	Enter the system priority value. The higher the value number the lower the priority. 1-65535 32768

Related Commands

Command	Description
lacp group	Enable LACP and configure on the interface.
show lacp	View the LACP configuration status.
show interface port-channel	View information on a specified port channel interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lACP timeout

```
lACP timeout {long | short}
```

Description

Configure the timeout period for the LACP session. The timeout value is the amount of time that a port-channel interface waits for LACP data units from the remote system before terminating the LACP session.

Parameter	Description
long	Enter the keyword long to set the LACP session to 90 seconds. This is the default.
short	Enter the keyword short to set the LACP session to 3 seconds.

Related Commands

Command	Description
lACP group	Enable LACP and configure on the interface.
show lACP	View the LACP configuration status.
show interface port-channel	View information on a specified port channel interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lc-rap-pool

lc-rap-pool <pool_name>

Description

This command is used to configure the Remote AP inner IP pool for cluster deployment.

Parameter	Description
pool_name	Specify the name of the local IP pool.
pool_start_address	Configure the start address of the local pool.
pool_end_address	Configure the end address of the local pool.

Example

To configure a Remote AP inner pool for cluster deployment, execute the command

```
(host) [mynode] (config) #lc-rap-pool rap-cluster 3.1.1.3 3.1.1.10
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lc-rap-pool-v6

lc-rap-pool-v6 <pool_name>

Description

This command is used to configure the Remote AP inner IPv6 pool for cluster deployment.

Parameter	Description
pool_name	Specify the name of the local IPv6 pool.
pool_start_address	Configure the start IPv6 address of the local pool.
pool_end_address	Configure the end IPv6 address of the local pool. NOTE: The maximum allowed size of the IPv6 pool is 64516.

Example

The following command assigns inner IPv6 pool to Remote APs to establish tunnel in a cluster deployment:

```
(host) [mynode] (config) #lc-rap-pool-v6 v6pool 2011::3 2011::10
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

lcd-menu

lcd-menu

```
[no] disable menu [maintenance [factory-default| media-eject| qui-quick-setup |  
media-eject | system-halt | system-reboot | upgrade-image [partition0 |  
partition1]| upload-config]]
```

Description

This command allows you to enable or disable the LCD menu either completely or for specific operations. You can use this command to disable executing the maintenance operations using the LCD menu. You can use the no form of these commands to enable the specific LCD menu.

Parameter	Description
lcd-menu	Enters the LCD menu configuration mode.
no	Delete the specified LCD menu option.
disable	Disables (or enables) the complete LCD menu.
maintenance	Disables (or enables) the maintenance LCD menu. Enabled
factory-default	Disables (or enables) the return to factory default option in the LCD menu. Enabled
media-eject	Disables (or enables) the media eject option in the LCD menu. Enabled
system-halt	Disables (or enables) the system halt option in the LCD menu. Enabled
system-reboot	Disables (or enables) the system reboot in the LCD menu. Enabled
upgrade-image	Disables (or enables) the upgrade image option in the LCD menu. Enabled
partition 0 partition 1	Disables (or enables) image upgrade on the specified partition (0 or 1). Enabled
upload-config	Disables (or enables) the upload config option in the LCD menu. Enabled

Example

The following example enables system halt and system reboot options:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #no disable menu maintenance system-halt
(host) [mynode] (lcd-menu) #no disable menu maintenance system-reboot
```

The following example disables the LCD menu completely:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #disable menu
```

The following example disables executing the specified maintenance operation using the LCD menu:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #disable menu maintenance ?
factory-default          Disable factory default menu
gui-quick-setup          Disable quick setup menu on LCD
media-eject              Disable media eject menu on LCD
system-halt              Disable system halt menu on LCD
system-reboot            Disable system reboot menu on LCD
upgrade-image            Disable image upgrade menu on LCD
upload-config            Disable config upload menu on LCD
(host) (lcd-menu) #disable menu maintenance upgrade-image ?
partition0               Disable image upgrade on partition 0
partition1               Disable image upgrade on partition 1
```

You can use the following show command to display the current LCD settings:

```
(host) [mynode]#show lcd-menu
lcd-menu
-----
Menu                               Value
----                               -
menu maintenance upgrade-image partition0  enabled
menu maintenance upgrade-image partition1  enabled
menu maintenance system-reboot reboot-stack  enabled
menu maintenance system-reboot reboot-local  enabled
menu maintenance system-halt halt-stack      enabled
menu maintenance system-halt halt-local      enabled
menu maintenance upgrade-image              enabled
menu maintenance upload-config              enabled
menu maintenance factory-default            enabled
menu maintenance media-eject                enabled
menu maintenance system-reboot              enabled
menu maintenance system-halt                enabled
menu maintenance gui-quick-setup            enabled
```

menu maintenance
menu

enabled
enabled

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
7200 Series controllers	Base operating system.	Config mode on Mobility Conductor.

license

```
license
  add <key>
  asp
  del <key>
  export <filename>
  import <filename>
  remote remote-ip-addr <ip-addr> add <key>
  report <filename>}
  server-ip <ip-addr> <ipv6-addr>
```

Description

This command allows you to install, delete, and manage software licenses on Mobility Conductor. ArubaOS supports a centralized licensing architecture, which allows a group of managed devices to share a pool of licenses. A primary and backup Mobility Conductor can share a single set of licenses, eliminating the need for a redundant license set on the backup server. Managed devices maintain information sent from the Mobility Conductor, even if the managed device and the Mobility Conductor can no longer communicate.

A Mobility Conductor uses licensing pools to distribute licenses to a large number of managed devices across geographic locations. By default, all managed devices associated to a Mobility Conductor share a single global pool of all the sharable licenses added to that Mobility Conductor. However, ArubaOS also allows you to create additional licensing pools at a configuration node, allowing a groups of managed devices at or below that configuration level to share licenses among themselves, but not with other groups. For information on creating license pools using the Mobility Conductor CLI, see [license-pool-profile](#).

New licenses and license pools can only be added through the Mobility Conductor WebUI. Licenses cannot be added directly to a managed devices. If a controller had previously installed sharable licenses before it was added to a Mobility Conductor as a managed devices, those licenses are no longer usable on that device. Those license keys must be regenerated and assigned to the **managed device** or licensing pool using the Mobility Conductor WebUI.

For complete information on the centralized licensing feature, refer to the *ArubaMobility ConductorLicensing Guide*.

Parameter	Description
add <key>	Installs the software license key in Mobility Conductor. The key is normally sent to you via email.
asp	Install Aruba Support Portal license This parameter is available in enable mode.
allocate-lic	Allocate licenses.

Parameter	Description
<code>get-allocated-lic</code>	Retrieves preallocated license keys from Aruba Support Portal.
<code>get-capacity-lic</code>	Get 9240 capacity license from Aruba Support Portal.
<code>get-md-pefv-lic</code>	Get MD PEFV license from Aruba Support Portal.
<code>register-order</code>	Register license order with Aruba Support Portal.
<code>export</code>	Exports the license database on Mobility Conductor to the specified file in flash.
<code>import</code>	Replaces the license database on Mobility Conductor with the specified file in flash. The system serial numbers referenced in the imported file must match the numbers on the Mobility Conductor.
<code>remote remote-ip-addr <ip-addr> add <key></code>	Use this command to associate a non-sharable license installed on the Mobility Conductor with the managed device for which that license key was generated. The <code><ip-addr></code> parameter is the IP address of the managed device, and <code><key></code> is the license key for the non-sharable license.
<code>report</code>	Saves a license report to the specified file in flash.
<code>server-ip <ip-addr> <ipv6-addr></code>	Enter the IPv4 or IPv6 address of the licensing server on a standalone controller or a Mobility Conductor to configure that controller as a licensing client. This command must be configured from the Mobility Conductor configuration node. NOTE: If there is an IPv4 address already configured on the controller, you must remove the IPv4 address before configuring the IPv6 address, and vice versa. If only IPv4 address is configured on the controller, it can only configure IPv4 license server IP address, and not IPv6 license server IP address.

Examples

From any configuration node , issue the command `license add <key>`.


```
(host)[mynode] #license add lnZSpC2vkLM1Jw8KVYdgj2
```

Related Commands

Command	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.6.0.0	The <ipv6-addr> sub-parameter was added to the <code>server-ip</code> parameter.
ArubaOS 8.2.0.0	The <code>server-ip</code> parameter can now associate multiple Mobility Conductors to a licensing server. In previous releases, this command was supported on standalone controllers only.
ArubaOS 8.0.1.0	The <code>server-ip</code> and <code>remote remote-ip-addr</code> parameters are introduced, and the <code>remote ip-addr</code> parameter is deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

license-pool-profile

```
license-pool-profile <profile>
  acr-licenses {eval key <key> <num>}|<num>
  ap-licenses {eval key <key> <num>}|<num>
  clone <source>
  license-pool-path <license-pool-path>
  mc-va-licenses-eg {eval key <key> <num>}|<num>}
  mc-va-licenses-il {eval key <key> <num>}|<num>}
  mc-va-licenses-jp {eval key <key> <num>}|<num>}
  mc-va-licenses-rw {eval key <key> <num>}|<num>}
  mc-va-licenses-us {eval key <key> <num>}|<num>}
  mm-license {eval key <key> <num>}|<num>}
  no
  pefng-licenses {eval key <key> <num>}|<num>}
  rfp-licenses {eval key <key> <num>}|<num>}
  via-licenses {eval key <key> <num>}|<num>}
  webcc-licenses {eval key <key> <num>}|{subscript key <key> <num>}}
```

Description

Use this command to create a local licensing pool and allocate licenses for that licensing pool. All managed devices associated to the same Mobility Conductor can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Conductor. However, ArubaOS also allows you to create individual licensing pools at a configuration node, allowing managed devices below that node to share licenses amongst themselves but not with other managed devices.



You must use the **license add** command to add license keys to the Mobility Conductor before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device.

For complete information on the centralized licensing feature, refer to the *Aruba Mobility Conductor Licensing Guide*.

Parameter	Description
<profile>	<p>The name of the profile for which you are creating a local license pool, for example, Northwest. The profile name is limited to 63 characters.</p> <p>NOTE: In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the <code>license-pool-path</code> parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less.</p>

Parameter	Description
acr-licenses	Add ArubaOS Advanced Cryptography (ACR) licenses to the selected pool. A license is required for each active client termination using Suite-B algorithms or protocols. Use the optional <code>eval key <key></code> parameters to specify an evaluation license key.
ap-licenses	Add AP licenses to the selected pool.
clone	Copy licenses from another license pool profile.
license-pool-path <license-pool-path>	Starting in ArubaOS 8.1.0.0, use this parameter to specify a license pool path, up to 255 characters, for example, /USA/northwest. NOTE: If you upgrade a legacy ArubaOS deployment to ArubaOS 8.1 or later, the license-pool-path parameter is automatically derived from the license-pool-profile <profile> name.
mc-va-licenses-eg mc-va-licenses-il mc-va-licenses-jp mc-va-licenses-rw mc-va-licenses-us	Add the following different MC-VA-XX license types enable APs to support regional channels for the following countries: <ol style="list-style-type: none"> 1. MC-VA-US: United states 2. MC-VA-JP: Japan 3. MC-VA-IL: Israel 4. MC-VA-EG: Egypt 5. MC-VA-RW: Rest of the world (all other countries)
mm-licenses	Add Mobility Conductor licenses to the selected pool.
pefng-licenses	Add PEF licenses to the selected pool to support PEF features, such as intelligent application identification, policy-based traffic management and controls, or stateful user firewalls.
rfp-licenses	Add RF Protect licenses to the selected pool, to support features such as spectrum analysis and WIP.
via-licenses	VIA licenses support VIA or 3rd party VPN client . VIA licenses are not consumed for site-to-site VPNs. If a managed device or standalone controller has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that device.
webcc-licenses	Add WebCC licenses to the selected pool. The WebCC license is a subscription-based, per-AP license.
[eval key <key>]	Use the optional <code>eval key <key></code> parameters to add the specified number of licenses for an evaluation license key.
<num>	Number of licenses supported by the license key.

Examples

```
(host)[mm] (config) #license-pool-profile Southwest
(host) ^[mm] (License pool profile "Southwest") #license-pool-path
/USA/southwest
(host) ^[mm] (License pool profile "Southwest") #ap-licenses 64
(host) ^[mm] (License pool profile "Southwest") #pefng-licenses 64
(host) ^[mm] (License pool profile "Southwest") #rfp-licenses 64
```

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.

Command History

Version	Description
ArubaOS 8.1.0.0	The <code>license-pool-path</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

license-pool-profile-root

```
license-pool-profile-root
  acr-license-enable
  no
  pefng-licenses-enable
  rfp-license-enable
  webcc-license-enable
```

Description

Use this command to enable shared license features within the global licensing pool. All managed devices associated to the same Mobility Conductor can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Conductor. Use this command to enable the functionality for a shared license functionality within these license pools.



Only AP licenses and VIA license are enabled by default when those licenses are added to Mobility Conductor, all other licenses must be manually enabled.

For complete information on the centralized licensing feature, refer to the *Aruba Mobility Conductor Licensing Guide*.

Parameter	Description
acr-license-enable	Enable ArubaOS Advanced Cryptography features. A license is required for each active client termination using Suite-B algorithms or protocols.
no ...	Include the no parameter before any license type to remove that configuration setting and disable licensing features for that license type.
pefng-licenses-enable	Enable PEF features, such as intelligent application identification, policy-based traffic management and controls, or stateful user firewalls.
rfp-license-enable	Enable RF Protect features, such as spectrum analysis and WIP.
webcc-license-enable	The Web Content Classification license is a subscription-based, per-AP license. Issue the <code>webcc-license-enable</code> command to enable web content classification features for the duration of the subscription period (up to 10 years per license)

Examples

From the SC configuration, issue the command `license-pool-profile-root acr-license-enable`.

```
(host) [MM] (config) #license-pool-profile-root
(host) [MM] (License root(/) pool profile) #acr-license-enable
```

Related Commands

Version	Description
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.

Command History

Version	Description
ArubaOS 8.2.0.0	The <code>xsc-license-enable</code> parameter was deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode from the MM configuration node on Mobility Conductor.

local-custom-cert

```
local-custom-cert local-mac <lmac> ca-cert <ca> server-cert <cert> load-balance  
suite-b <gcm-128 | gcm-256>
```

Description

This command configures the user-installed certificate for secure communication between a managed device and a Mobility Conductor.

Use this command on a Mobility Conductor to configure the custom certificate for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and certificates for the Mobility Conductor. If your Mobility Conductor and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2. When a managed device communicates with the Mobility Conductor to set up IPsec tunnels, the uplink vlan tag configured via the [uplink](#) command will be sent along in the vendor-id payload during IKE negotiation. This will uniquely bind the tunnel from a particular uplink on the managed device to a corresponding map on Mobility Conductor.

Parameter	Description
<lmac>	MAC address of the managed device with a local custom certificate.
ca-cert <ca>	User-defined name of a trusted CA certificate installed on the managed device. Use the <code>show crypto-local pki TrustedCA</code> command to display the CA certificates that have been imported into the managed device.
server-cert <cert>	User-defined name of a server certificate installed on the managed device. Use the <code>show crypto-local pki ServerCert</code> command to display the server certificates that have been imported into the managed device.
suite-b	If you configure your Mobility Conductor to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: <ul style="list-style-type: none">▪ gcm-128 Use 128-bit AES-GCM Suite-B encryption▪ gcm-256 Use 256-bit AES-GCM Suite-B encryption

Example

The following command configures the managed device with a user-installed certificate:

```
(host) [mynode] (config) #local-custom-cert local-mac 00:16:CF:AF:3E:E1 ca-  
cert cacert1 server-cert servercert1
```

Related Commands

Command	Description
show local-cert-mac	Display the IP, MAC address and certificate configuration of managed devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	The suite-b gcm-128 and suite-b gcm-256 encryption options for IPsec custom certificates requires the Advanced Cryptography license. All other parameters are available in the base operating system.	Config mode on Mobility Conductor.

local-factory-cert

```
local-factory-cert local-mac <lmac> [load-balance]
```

Description

This command configures the factory-installed certificate for communication between a managed device and a Mobility Conductor. Use this command on a Mobility Conductor to configure the factory certificate for communication with a managed device. On the managed device, use the `masterip` command to configure the IP address and certificates for the Mobility Conductor. If your Mobility Conductor and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2. When a managed device communicates with Mobility Conductor to set up IPsec tunnels, the uplink vlan tag configured via the [uplink](#) command will be sent along in vendor-id payload during IKE negotiation. This will uniquely bind the tunnel from a particular uplink on the managed device to a corresponding map on Mobility Conductor.

Parameter	Description
<lmac>	MAC address of the managed device with a local certificate.

Example

The following command configures the managed device with a factory-installed certificate:

```
(host)[node](config) #local-factory-cert local-mac 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description
show local-cert-mac	Display the IP, MAC address and certificate configuration of managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Conductor.

localip

```
localip <ipaddr>  
    ipsec <key>
```

Description

This command configures the IP address and preshared key for the managed device on a Mobility Conductor. Use this command on a Mobility Conductor to configure the IP address and preshared key or certificates for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and preshared key for the Mobility Conductor.

If your Mobility Conductor and managed devices use a PSK for authentication, they will create the IPsec tunnel using IKEv1.

Parameter	Description
<ipaddr>	IP address of the managed device. Use the 0.0.0.0 address to configure a global preshared key for all inter-managed device communications.
ipsec <key>	To establish the master/conductor-local IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.

Example

The following command configures the managed device with a PSK:

```
(host) [mynode] (config) #localip 0.0.0.0 ipsec gw1234xyz
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

localipv6

```
localipv6 <local-switch-ipv6>  
    ipsec <key>
```

Description

This command configures the IP address and preshared key for the managed device on a Mobility Conductor. Use this command on a Mobility Conductor to configure the IP address and preshared key or certificates for communication with a managed device. On the managed device, use the `masterip` command to configure the IP address and preshared key for the Mobility Conductor.

If your Mobility Conductor and managed devices use a PSK for authentication, they will create the IPsec tunnel using IKEv1.

Parameter	Description
<local-switch-ipv6>	IP address of the managed device. Use the 0.0.0.0 address to configure a global PSK for communication between managed devices.
ipsec <key>	To establish the master/conductor-local IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
localipv4 <localipv4_val>	IPv4 address of the managed device. NOTE: The configuration of the <code>localipv4 <localipv4_val></code> sub-parameter is optional in a native IPv6 deployment.

Example

The following command configures the managed device with a PSK:

```
(host) [mynode] (config) #localipv6 2001:0000:0eab:DEAD:0000:00AO:ABCD:004E  
ipsec gw1234xyz
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The <code>localipv4 <localipv4_val></code> sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

local-peer-mac

```
local-peer-mac <local-mac-addr> ipsec <localkey>
```

Description

This command is used to configure security peer-mac based between Mobility Conductor and managed devices.

Parameter	Description
<local-mac-addr>	Enter the managed device's MAC address.
ipsec <localkey>	Configure the value of the IKE PSK, it must be between 6-64 characters

Example

The following command configures the security peer-mac:

```
(host) [mynode] (config) #local-peer-mac 00:0c:29:00:00:00 ipsec 123456
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

local-userdb add

```
local-userdb add
  generate-username {generate-password|password <passwd>}
  comments
  email
  expiry
  guest-company
  guest-fullname
  guest-phone
  mode
  opt-field-1
  opt-field-2
  opt-field-3
  opt-field-4
  remote-ip
  role
  sponsor-dept
  sponsor-email
  sponsor-fullname
  sponsor-name
  start-time
username <name> {generate-password|password <passwd>}
  comments
  email
  expiry
  guest-company
  guest-fullname
  guest-phone
  mode
  opt-field-1
  opt-field-2
  opt-field-3
  opt-field-4
  remote-ip
  role
  sponsor-dept
  sponsor-email
  sponsor-fullname
  sponsor-name
  start-time
```

Description

This command creates a user account entry in Mobility Conductor's internal database. When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the `local-userdb modify` command, or delete an account with the `local-userdb del` command.

By default, the internal database in Mobility Conductor is used for authentication. Issue the `aaa authentication-server internal use-local-switch` command to use the internal database in

a managed device; you then need to add user accounts to the internal database in the managed device.

Parameter	Description
generate-username	Automatically generate and add a username.
username	Add the specified username. 1-64 characters
generate-password	Automatically generate a password for the username.
password	Add the specified password for the username. 6-128 characters
comments	Comments added to the user account.
email	Email address for the user account.
expiry	Expiration for the user account. If this is not set, the account does not expire. no expiration
duration	Duration, in minutes, for the user account. 1-2147483647
time	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.
guest-company	Name of the guest's company. NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
mode	Enables or disables the user account. disabled
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .

Parameter	Description
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
remote-ip	IP address assigned to the remote peer.
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method. guest
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.
sponsor-fullname	The sponsor's full name.
sponsor-name	The sponsor's name.
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.

Example

The following command adds a user account in the internal database with an automatically-generated username and password:

```
(host) [mynode] #local-userdb add generate-username generate-password expiry
duration 480
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest4157
Password: cDFD1675
Expiration: 480 minutes
```

Related Commands

Command	Description
mgmt-user	Use the <code>webui-cacert <certificate name></code> command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated. Use the <code>mgmt-user webui-cacert <certificate_name> serial <number> <username> <role></code> command if you want the authentication process to use previously configured certificate name and serial number to derive the user role.
show local-userdb	Use this command to show the parameters displayed in the output of this command.
show local-userdb-guest	Use this command to show the parameters displayed in the output of the local-userdb-guest add command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb del

```
local-userdb
  del username <name>
    comments
    email
    expiry
    guest-company
    guest-fullname
    guest-phone
    mode
    opt-field-1
    opt-field-2
    opt-field-3
    opt-field-4
    remote-ip
    role
    sponsor-dept
    sponsor-email
    sponsor-fullname
    sponsor-name
    start-time
del-all
```

Description

This command deletes entries in the Mobility Conductor's internal database. User account entries created with expiration are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Parameter	Description
del username	Deletes the user account for the specified username.
comments	Comments added to the user account.
email	Email address for the user account.
expiry	Expiration for the user account. If this is not set, the account does not expire. no expiration NOTE: This parameter is available only for AOS version 8.6 or earlier.
duration	Duration, in minutes, for the user account. 1-2147483647

Parameter	Description
time	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.
guest-company	Name of the guest's company. NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
mode	Enables or disables the user account. disabled NOTE: This parameter is available only for AOS version 8.6 or earlier.
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
remote-ip	IP address assigned to the remote peer. NOTE: This parameter is available only for AOS version 8.6 or earlier.
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method. guest
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.

Parameter	Description
sponsor-fullname	The sponsor's full name.
sponsor-name	The sponsor's name.
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins. NOTE: This parameter is available only for AOS version 8.6 or earlier.
del-all	Deletes all entries in the internal database.

Example

The following command deletes a specific user account entry:

```
(host) [mynode] #local-userdb del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb export

```
local-userdb export <filename>
```

Description

This command exports the internal database to a file. After using this command, you can use the `copy` command to transfer the file from flash to another location.



Use this command with caution. It replaces the existing users with user entries from the imported file.

Parameter	Description
export	Saves the internal database to the specified file in flash.

Example

The following command saves the internal database to a file:

```
(host) [mynode] #local-userdb export jan-userdb
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform s	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb import

```
local-userdb import <filename>
```

Description

This command replaces the internal database with the specified file from flash. This command replaces the contents of the internal database with the contents in the specified file. The file must be a valid internal database file saved with the `local-userdb export` command.

Parameter	Description
<code>import</code>	Replaces the internal database with the specified file.

Example

The following command imports the specified file into the internal database:

```
(host) [mynode] #local-userdb import jan-userdb
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb modify

```
local-userdb modify username <name>
  comments
  email
  expiry
  guest-company
  guest-fullname
  guest-phone
  mode
  opt-field-1
  opt-field-2
  opt-field-3
  opt-field-4
  remote-ip
  role
  sponsor-dept
  sponsor-email
  sponsor-fullname
  sponsor-name
  start-time
```

Description

This command modifies an existing user account entry in the Mobility Conductor's internal database. Use the `show local-userdb` command to view the current user account entries in the internal database.

Parameter	Description
<code>username</code>	Name of the existing user account entry. 1-64 characters
<code>comments</code>	Comments added to the user account.
<code>email</code>	Email address for the user account.
<code>expiry</code>	Expiration for the user account. If this is not set, the account does not expire. no expiration
<code>duration</code>	Duration, in minutes, for the user account. 1-2147483647
<code>time</code>	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.
<code>guest-company</code>	Name of the guest's company.

Parameter	Description
	NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
mode	Enables or disables the user account. disabled
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
remote-ip	IP address assigned to the remote peer.
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method. guest
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.
sponsor-fullname	The sponsor's full name.
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.

Example

The following command disables an existing user account in the internal database:

```
(host) [mynode] #local-userdb modify username guest4157 mode disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb-guest add

```
local-userdb-guest
local-userdb-guest add
  generate-username {generate-password|password <passwd>}
  comments
  email
  expiry
  guest-company
  guest-fullname
  guest-phone
  mode
  opt-field-1
  opt-field-2
  opt-field-3
  opt-field-4
  remote-ip
  role
  sponsor-dept
  sponsor-email
  sponsor-fullname
  sponsor-name
  start-time
username <name> {generate-password|password <passwd>}
  comments
  email
  expiry
  guest-company
  guest-fullname
  guest-phone
  mode
  opt-field-1
  opt-field-2
  opt-field-3
  opt-field-4
  remote-ip
  role
  sponsor-dept
  sponsor-email
  sponsor-fullname
  sponsor-name
  start-time
```

Description

This command creates a guest user in a local user database. When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the `local-userdb-guest modify` command, or delete an account with the `local-userdb-guest del` command. By default, the internal database in the Mobility Conductor is used for authentication. Issue the `aaa authentication-server internal use-local-switch` command to use the

internal database in a managed device you then need to add user accounts to the internal database in the managed device.

Parameter	Description
generate-username	Automatically generate and add a guest username.
username	Add the specified guest username. 1-64 characters
generate-password	Automatically generate a password for the username.
password	Add the specified password for the username. 6-128 characters
comments	Comments added to the user account.
email	Email address for the user account.
expiry	Expiration for the user account. If this is not set, the account does not expire. no expiration
duration	Duration, in minutes, for the user account. 1-2147483647
time	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.
guest-company	Name of the guest's company. NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
mode	Enables or disables the user account. disabled
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .

Parameter	Description
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
remote-ip	IP address assigned to the remote peer. NOTE: This parameter is available only for AOS version 8.6 or earlier.
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method. guest NOTE: This parameter is available only for AOS version 8.6 or earlier.
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.
sponsor-fullname	The sponsor's full name.
sponsor-name	The sponsor's name.
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.

Example

The following command adds a guest user in the internal database with an automatically-generated username and password:

```
(host) [mynode] #local-userdb-guest add generate-username generate-password
expiry none
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest-5433352
Password: mBgJ6764
Expiration: none
```

Related Commands

Command	Description
<u>show local-userdb-guest</u>	Show the parameter configured using the <code>local-userdb-guest</code> command.
<u>show local-userdb</u>	Show the parameters configured using the <code>local-userdb</code> command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system. The <code>role</code> parameter requires the PEFNG license.	Enable mode on Mobility Conductor.

local-userdb-guest del

```
local-userdb-guest {del username <name> | del-all}
```

Description

This command deletes entries in the controller's internal database. User account entries created with expiration detail are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Parameter	Description
del username	Deletes the user account for the specified username.
comments	Comments added to the user account.
email	Email address for the user account.
grantor	Change the grantor of the guest user entry
guest-company	Name of the guest's company. NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.

Parameter	Description
sponsor-fullname	The sponsor's full name.
sponsor-name	The sponsor's name.
del-all	Deletes all entries in the internal database.

Example

The following command deletes a specific user account entry:

```
(host) #local-userdb-guest del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and config modes on Mobility Conductor.

local-userdb-guest modify

```
local-userdb-guest modify username <name> [comments <g_comments>][email <email>]
[expiry {duration <minutes>|time <mm/dd/yyyy> <hh:mm>}] [guest-company <g_company>]
[guest-fullname <g_fullname>][guest-phone <g-phone>][mode disable][opt-field-1
<opt1>][opt-field-2 <opt2>][opt-field-3 <opt3>][opt-field-4 <opt4>][password
<passwd>][sponsor-dept <sp_dept>][sponsor-mail <sp_email>][sponsor-fullname <sp_
fullname>][sponsor-name <sp_name>][start-time <mm/dd/yyyy> <hh.mm>]
```

Description

This command modifies an existing guest user entry in the controller's internal database. Use the **show local-userdb-guest** command to view the current user account entries in the internal database.

Parameter	Description
username	Name of the existing user account entry. 1-64 characters
comments	Comments added to the user account.
email	Email address for the user account.
expiry	Expiration for the user account. If this is not set, the account does not expire. no expiration
grantor	Change the grantor of the guest user entry
duration	Duration, in minutes, for the user account. 1-2147483647
time	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.
guest-company	Name of the guest's company. NOTE: A guest is the person who needs guest access to the company's Aruba wireless network.
guest-fullname	The guest's full name.
guest-phone	The guest's phone number.
mode	Enables or disables the user account. Disable

Parameter	Description
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.
opt-field-2	Same as opt-field-1 .
opt-field-3	Same as opt-field-1 .
opt-field-4	Same as opt-field-1 .
password	User's password. 1-6 characters
sponsor-dept	The guest sponsor's department name. NOTE: A sponsor is the guest's primary contact for the visit.
sponsor-email	The sponsor's email address.
sponsor-fullname	The sponsor's full name.
sponsor-name	The sponsor's name.
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.

Example

The following command disables a guest user account in the internal database:

```
(host) #local-userdb-guest modify username guest4157 mode disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and config modes on Mobility Conductor.

local-userdb-guest send-email

```
local-userdb-guest send-email <username> [to-guest][to-sponsor]
```

Description

This command causes the controller to send email to the guest or sponsor any time a guest user is created. This command ensures that the controller sends an email to the guest or sponsor any time a guest user is created.

Parameter	Description
<username>	Name of the guest. 1-64 characters
to-guest	Allows you to send email to the guest user's address.
to-sponsor	Allows you to send email to the sponsor's email address.

Example

The following command causes the controller to send an email to the sponsor alerting them that the guest user **Laura** was just created.

```
(host)# local-userdb-guest send-email Laura to-sponsor
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb-public-access

```
local-userdb
  del username <name>
  del-all
```

Description

This command deletes guest entries in the Mobility Conductor's internal database. User account entries created with expiration are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Parameter	Description
del username	Deletes a guest user account for the specified username.
del-all	Deletes all guest entries in the internal database.

Example

The following command deletes a specific guest account entry:

```
(host) [mynode] #local-userdb-public-access del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

local-userdb maximum-expiration

```
local-userdb maximum-expiration <expmins>
```

Description

This command configures the maximum time, in minutes, that a guest account in the internal database can remain valid. The user in the guest-provisioning role cannot create guest accounts that expire beyond the configured maximum time. This command is not available to the user in the guest-provisioning role.

Parameter	Description
maximum-expiration	Maximum time, in minutes, that a guest account in the internal database can remain valid. 1-3000000

Example

The following command sets the maximum time for guest accounts in the internal database to 8 hours (480 minutes):

```
(host) [/md] (config) #local-userdb maximum-expiration 480
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

local-userdb send-to-guest

local-userdb send-to-guest

Description

This command automatically sends email to the guest when the guest user is created.

A guest is the person who needs guest access to the company's Aruba wireless network. Email is sent directly to the guest after the guest user is created. When configuring the guest provisioning feature, the guest user is generally created by Guest Provisioning user. This is the person who is responsible for signing in guests at your company.

Example

```
(host) [mynode] (config) #local-userdb send-to-guest
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

local-userdb send-to-sponsor

local-userdb send-to-sponsor

Description

This command automatically sends email to the guest's sponsor when the guest user is created. The sponsor is the guest's primary contact. Email is sent directly to the guest's sponsor after the guest user is created. When configuring the guest provisioning feature, the sponsor is generally created by the Guest Provisioning user. This is the person who responsible for signing in guests at your company.

Example

```
(host) [mynode] (config)#local-userdb send-to-sponsor
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

location

location <switchlocation>

Description

This command configures the location of the managed device. Use this command to indicate the location of the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter "" at the prompt.

Parameter	Description
switchlocation	A text string that specifies the location of the switch.

Example

The following command configures the location:

```
(host) [mynode] (config) #location "Building 10, second floor, room 21E"
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

location-server-feed

enable
disable

Description

This command sends RSSI information from APs to a location management server, which can use that information to compute the location of stations seen in the network.

Parameter	Description
enable	Enable the feed that sends RSSI information to a location management server. This feature is disabled by default.
disable	Disable the feed that sends RSSI information to a location management server. This feature is disabled by default.

Example

The following command configures the location:

```
(host) [mynode] (config) #location-server-feed enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

logging

```
logging [ap-debug|arm|arm-user-debug|facility|network|peer-  
debug|security|system|user|user-debug|wireless|<ipv4addr>|<ipv6addr>]
```

Description

Use this command to specify the IP address of the remote logging server, facility, severity, and the type. The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages. Use the [show logging](#) command to verify that the device sends logging messages.

There are eight logging severity levels, each with its associated types of messages. Each level also includes the levels below it. For example, if you set the logging level to informational (6), all messages from level 0 through level 5 (from emergencies through notifications) are also logged. The warnings severity level is set by default for all message categories.

Only the **logging level warnings security subcat ids** and **logging level warnings security subcat ids-ap** subcategories are enabled by default. Other subcategories are not generated by default even their severity is **warning** or higher.

Parameter	Description
ap-debug <name>	AP troubleshooting messages. You must specify a debug value.
arm level process subcat	ARM messages.
arm-user-debug <mac>	ARM user troubleshooting messages. You must specify a MAC address.
facility	Set the facility to be used when logging to the remote syslog server. The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages. local 0 to local 7
network level process subcat	Network messages.
peer-debug <mac>	Peer Debug Logs.
security level	Security messages.

Parameter	Description
process subcat	
system level process subcat	System messages.
user level process subcat	User messages.
user-debug <mac>	User troubleshooting messages. You must specify a MAC address.
wireless level process subcat	Wireless messages.
<ipv4addr>	To set the remote logging server IPv4 address. A.B.C.D
dest-port <destination-port>	Select destination port for Syslog messages to this IP address.
facility	The facility to be used when logging to a remote syslog server. local 0 to local 7
format	The format of the logs when logging to a remote syslog server. <ul style="list-style-type: none"> ▪ cef - Common Event Fformat ▪ bsd-standard - Berkeley Software Distribution standard or RFC-3164 format
severity	Set the remote logging server severity to: <ul style="list-style-type: none"> ▪ alerts - Immediate action required ▪ critical - Critical Condition ▪ debugging - Debug Messages ▪ emergencies - System is unusable ▪ errors - Error Conditions in the system ▪ informational - Informational Messages ▪ notifications - Normal but significant condition ▪ warnings - Warning condition
source-interface <VLAN number>	Select source address of outgoing Syslog messages.

Parameter	Description
tls	Enable TLS option for rsyslog.
type	Set the remote logging server message type to: <ul style="list-style-type: none"> ▪ ap-debug - AP Debug Logs ▪ arm - ARM logs ▪ arm-user-debug - ARM User Debug Logs ▪ network - Network logs ▪ security - Security logs ▪ system - System logs ▪ user - User logs ▪ user-debug - User Debug Logs ▪ wireless - Wireless logs
<ipv6addr>	To set the remote logging server IPv6 address. X:X:X:X::X
dest-port <destination-port>	Select destination port for Syslog messages to this IP address.
facility	The facility to be used when logging to a remote syslog server. local 0 to local 7
format	The format of the logs when logging to a remote syslog server. <ul style="list-style-type: none"> ▪ cef - Common Event Fformat ▪ bsd-standard - Berkeley Software Distribution standard or RFC-3164 format
severity	Set the remote logging server severity to: <ul style="list-style-type: none"> ▪ alerts - Immediate action required ▪ critical - Critical Condition ▪ debugging - Debug Messages ▪ emergencies - System is unusable ▪ errors - Error Conditions in the system ▪ informational - Informational Messages ▪ notifications - Normal but significant condition ▪ warnings - Warning condition
type	Set the remote logging server message type to: <ul style="list-style-type: none"> ▪ ap-debug - AP Debug Logs ▪ arm - ARM logs ▪ arm-user-debug - ARM User Debug Logs ▪ network - Network logs ▪ security - Security logs ▪ system - System logs

Parameter	Description
	<ul style="list-style-type: none"> ▪ user- User logs ▪ user-debug - User Debug Logs ▪ wireless - Wireless logs
level	<p>The message severity level, which can be one of the following (in order of severity level):</p> <ul style="list-style-type: none"> ▪ alerts - Any condition requiring immediate attention and correction. ▪ critical - Any critical conditions, such as hard drive errors. ▪ debugging - Messages containing information for debugging purposes. ▪ emergencies - Panic conditions that occur when the system becomes unstable. ▪ errors - Error conditions. ▪ informational - Significant events of a non-critical and normal nature. ▪ notifications - Normal but significant condition. ▪ warnings - Warning messages.
process	<p>controller process, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ aaa - AAA logging ▪ activate - Integration and communication with an Activate server ▪ amon_recvr - AMON receiver ▪ amon_sender - AMON sender ▪ apprf - APPRF feature ▪ approc - AP processes ▪ armd - ARM processes ▪ authmgr - User authentication ▪ ble_relay - BLE relay process ▪ bocmgr - BOC manager process ▪ cert_dwnld - Certificate download process ▪ certmgr - Certificate manager ▪ cfgdist - Config Distributor ▪ cfgm - Configuration Manager ▪ cli - Command Line Interface ▪ cluster_mgr - Cluster Manager ▪ cpsec - Control plane security ▪ crypto - VPN (IKE/IPsec) ▪ cts - Transport service ▪ dbsync - Database synchronization ▪ dds - Logging for DDS processes ▪ dhcpd - DHCP packets ▪ dpagent - DPAGENT process

Parameter	Description
	<ul style="list-style-type: none"> ▪ esi - External Services Interface ▪ extifmgr - External Interface Manager ▪ fpapps - Layer 2 and 3 control ▪ fw_visibility - Firewall visibility processes ▪ gsmmgr - GSM manager ▪ ha_mgr - High availability manager ▪ hcm - Health check process ▪ httpd - Apache process ▪ hwmon - Hardware monitoring ▪ iapmgr - Instant AP manager process ▪ ip_flow_export - IP Flow Export process ▪ ipstm - Instant station manager process ▪ l2tp - L2TP ▪ lagm - Logging for lagm process ▪ licensmgr - License manager ▪ lldp - LLLDP process ▪ localdb - Local database ▪ mdns - Multicast DNS proxy ▪ mobileip - Mobile IP ▪ mon_serv - mon_serv process ▪ mon_serv_fwv - mon_serv_fwv process ▪ npppd - NPPPD ▪ ofa - OpenFlow Agent Process ▪ ospf - OSPF logging ▪ packetfilter - Packet filtering of messaging and control frames ▪ phonehome - PhoneHome ▪ pim - Protocol Independent Multicast ▪ pppd - PPP ▪ pppoe - PPPoE ▪ pptp - PPTP ▪ processes - Run-time process ▪ profmgr - Profile Manager ▪ publisher - Publish subscribe service ▪ radvd - RA daemon ▪ resolvwrap - Resolve wrap process ▪ rfm - RF Troubleshooting Manager ▪ rng_mgr - RNG Manager ▪ rsync - Rsync ▪ rtpa - RTPA process ▪ sc_replication_mgr - SC Replication Manager ▪ snmp - SNMP ▪ spectrum - Spectrum analysis processes ▪ stm - Station management ▪ survival - Auth survival

Parameter	Description
	<ul style="list-style-type: none"> ▪ syslogdwrap - Syslogd wrap ▪ traffic - Traffic process ▪ ucm - Unified Communication and Collaboration processes ▪ upgrademgr - Upgrade Manager ▪ util-proc - Util process ▪ vrrp - Logging for vrrp process ▪ web_cc - Web Content classification ▪ webd - Web Daemon. ▪ wms - Wireless management
subcat	<p>Message subcategory, which depends upon the message category specified. The following lists the subcategories available for each message category:</p> <ul style="list-style-type: none"> ▪ ap-debug: all, ap-config, ha, sdn ▪ arm: all, client-match, radio-mgmt ▪ arm-user-debug: all ▪ network: all, cluster, dhcp, gp, mobility, packet-dump, sdn ▪ security: aaa, all, auth-amon, certinit, certmgr, cluster, cpnw, cpsec, db, 802.1X, firewall, HA, ids, ids-ap, kerberos, mobility, packet-trace, vpn, webserver, wl-sync ▪ system: all, amon, amon-ale, amon-amp, ap, ap-config, cluster, configuration, cpnw, gp, ha, mapc, messages, ofc-event-dispatcher, ofc-flow-manager, ofc-packet-dispatcher, ofc-routing-switch, ofc-switch-manager, ofc-topology, ofc-topology-discovery, pan, reg-tbl, snmp, validation, webserver ▪ user: all, captive-portal, client-match, cpnw, 802.1X, mapc, pan, radius, vpn ▪ user-debug: all, configuration ▪ wireless: all

Example

The following command adds the remote logging server with the IP address 10.1.2.3 with a user log type using local4.

```
(host) [mynode] (config) #logging 10.1.2.3 facility local4
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>tls</code> subparameter was introduced.
ArubaOS 8.7.0.0	The <code>peer-debug</code> parameter was introduced.
ArubaOS 8.2.0.0	New system processes called vrrp and lagm were added to debug issues related to the <code>vrrp</code> process and <code>lagm</code> process.
ArubaOS 8.1.0.0	The logging level <severity> was moved to the end of the command string. The <code>format</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

logging-trace-files

logging-trace-files

Description

Use this command to enable or disable the slog_flash application. The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Example

The following command disables slog_flash app.

```
(host) [mynode] #no logging-trace-files
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
7200 Series, 7030, and 7010	Base operating system.	Config mode on Mobility Conductor.

login session

login session timeout <minutes>

Description

This command configures the time management session (via Telnet or SSH) remains active without user activity. The management user must re-login to the controller after a Telnet or SSH session times out. If you set the timeout value to 0, sessions do not time out. The TCP session timeout for wireless and wired user sessions through the controller is 15 minutes; this timeout for user sessions is not configurable.

Parameter	Description
timeout	Number of seconds or minutes that a management session remains active without any user activity. 1-60 minutes or 5-3600 seconds, 0 to disable 15 minutes

Example:

The following command configures management sessions on the controller to not time out:

```
(host) [mynode] (config) #login session timeout 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

logon

logon <device-ip>

Description

This command remotely logs in to the managed device CLI from the Mobility Conductor CLI. Ensure that the managed device is reachable from Mobility Conductor.

Parameter	Description
device-ip	IP address of the managed device.

Example

This command remotely logs in to the managed device CLI from the Mobility Conductor CLI.

```
(host) [mynode] (config) #logon 192.0.2.38
Last login: Wed Jun 29 08:23:33 2016 from 192.0.2.34
(host-md) #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

mac-address-table

```
mac-address-table static <macaddr> gigabitethernet <slot/module/port> vlan <vlan>
```

Description

This command adds a static entry to the MAC address table. The MAC address table is used to forward traffic between ports on the controller. The table includes addresses learned by the controller. This command allows you to manually enter static addresses that are bound to specific ports and VLANs.

Parameter	Description
<macaddr>	MAC address, in the format xx:xx:xx:xx:xx:xx.
<slot/module/port>	Interface in <slot>/<module>/<port> format.
vlan	ID number of the VLAN. 1-4094

Example

The following command configures a MAC address table entry:

```
(host) [mynode] (config) #mac-address-table static 00:0b:86:f0:05:60  
gigabitethernet 0/0/12 vlan 22
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Conductor.

managed-device delete image

```
managed-device delete image  
  all  
  image_name
```

Description

This command deletes the image stored in Mobility Conductor file system.

Parameter	Description
all	This parameter deletes all the images.
image_name	This parameter deletes a specific image in the Mobility Conductor file system.

Related Commands

Command	Description
show managed-device images	This command displays the images of managed devices stored in the Mobility Conductor file server.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and managed device.

master-l3redundancy/conductor-l3redundancy

```
master-l3redundancy/conductor-l3redundancy
l3-peer-ip-address {[<ipv4-addr>|<ipv6-addr>]} [ipsec <key>] [ipsec-custom-cert
<peer-mac> <MAC address> {ca-cert <certificate> | peer-mac-2 <MAC address>}]
[ipsec-factory-cert <peer-mac> <MAC address>]}
l3-sync-state {None|Primary|Secondary}
l3-sync-time <timer>
no...
```

Description

Use this command to configure and enable Layer-3 redundancy for a Mobility Conductor. Peer-ip and sync-state functions are required for proper functioning of Layer-3 redundancy. They have to be individually executed in **/mm/mynode** of all the Mobility Conductors involved in the redundancy.

Parameter	Description
l3-peer-ip-address	Configure L3 peer's ip address.
<ipv4-addr>	Configure ipv4 address of the peer Mobility Conductor.
<ipv6-addr>	Configure ipv6 address of the peer Mobility Conductor.
ipsec	Configure IPsec secure communication between Mobility Conductors.
ipsec-custom-cert	Customer certificate-based IPsec secure communication between Mobility Conductors.
ipsec-factory-cert	Factory certificate-based IPsec secure communication between Mobility Conductors.
l3-sync-state	Sync state for L3 Redundancy .
None	No Sync state for L3 Redundancy.
Primary	Set Sync state for L3 Redundancy as Primary.
Secondary	Set Sync state for L3 Redundancy as Secondary.
l3-sync-time	Sync Time for L3 Redundancy.
timer	Sync time in Hours. Value is between (2-24) hours. 2 hours
no	Negates any configured parameter.

Example

The following command enables you to configure Layer-3 redundancy.

```
(host) *[mynode] (config) #master-l3redundancy/conductor-l3redundancy
(host) *[mynode] (config-submode)# #l3-peer-ip-address
(host) *[mynode] (config-submode)#l3-sync-state
(host) *[mynode] (config-submode)#l3-sync-time
```

The following example configures Layer-3 redundancy for IPv6 address using custom-installed certificate on the Mobility Conductors:

```
(host) *[mynode] (config) #master-l3redundancy/conductor-l3redundancy
(host) *[mynode] (config-submode)# #l3-peer-ip-address 2021:1:1:166::254
ipsec-custom-cert peer-mac 00:0c:29:42:4c:b6 ca-cert L3-Primarysecondary-
CA server-cert L3-Secondary suite-b gcm256
```

The following example configures Layer-3 redundancy for IPv6 address using factory-installed certificate on the Mobility Conductors:

```
(host) *[mynode] (config) #master-l3redundancy/conductor-l3redundancy
(host) *[mynode] (config-submode)# #l3-peer-ip-address 2001:78::245 ipsec-
factory-cert peer-mac 20:4c:03:0e:e1:68
```

The following example configures Layer-3 redundancy for IPv6 address using IPsec secure communication between the Mobility Conductors:

```
(host) *[mynode] (config) #master-l3redundancy/conductor-l3redundancy
(host) *[mynode] (config-submode)# #l3-peer-ip-address 2021:1:1:145::109
ipsec itsabug
```

Related Commands

Command	Description
show master-l3redundancy/show conductor-l3redundancy	Displays the current status of Layer-3-domain Mobility Conductor redundancy.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The <code><ipv6-addr></code> sub-parameter was added.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on managed device.

master-redundancy master-vrrp/conductor-redundancy conductor-vrrp

```
master-redundancy/conductor-redundancy
master-vrrp/conductor-vrrp [ipv6 | <id>]
no...
peer-ip-address [ipv6 <X:X:X:X::X>|ipv4]
```

Description

This command associates a VRRP instance with Mobility Conductor redundancy. To maintain a highly redundant network, you can use a standby Mobility Conductor. The underlying protocol used is VRRP, which you configure using the `vrrp` command.

Parameter	Description
<code>master-vrrp/conductor-vrrp</code>	Configure the virtual router ID of the master/conductor switch.
<code>ipv6</code>	The VRRP IPv6 address to establish an IPv6 IPsec tunnel.
<code><id></code>	The virtual router ID for the VRRP instance configured with the <code>vrrp</code> command. 1-255
<code>no</code>	Negates any configured parameter.
<code>peer-ip-address <ipv6 ipv4></code>	Configure peer IPv4 or IPv6 address.

Example

The following command configures VRRP IPv4 address for the initially preferred Mobility Conductor:

```
(host)[mynode](config) #vrrp 22
vlan 22
ip address 10.200.22.254
priority 110
preempt
description Preferred-Master/Conductor
tracking master-up-time//conductor-up-time 30 add 20
no shutdown
master-redundancy/conductor-redundancy
master-vrrp/conductor-vrrp 22
peer-ip-address 192.168.2.1 ipsec qwerty012
```

The following shows the corresponding VRRP IPv4 address configuration for the peer controller.

```
(host)[mynode](config) #vrrp 22
vlan 22
ip address 10.200.22.254
priority 100
preempt
description Backup-Master/Conductor
tracking master-up-time/conductor-up-time 30 add 20
no shutdown
master-redundancy/conductor-redundancy
master-vrrp/conductor-vrrp 22
peer-ip-address 192.168.22.1 ipsec qwerTY012
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The <code>ipv6 <ipv6-addr></code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

masterip/conductorip

```
masterip / conductorip<ipaddr>  
  ipsec <key> [fqdn <local-fqdn>] interface <uplink |{vlan <id>}] peer-mac-1  
  <peermac1  
  ipsec-custom-cert master-mac-1-c <mac-1-c> ca-cert <ca> fqdn <fqdn> [interface  
  uplink|{vlan <id>}] [master-mac-2-c <mac-2-c>] server-cert <cert> [suite-b gcm-  
  128|gcm-256]  
  ipsec-factory-cert master-mac-1 <mac>  
  vpn-ip <vpnip> {ipsec|ipsec-custom-cert|ipsec-factory-cert}  
  web-socket-acp
```

Description

This command configures the IP address and PSK or certificate for the Mobility Conductor on a managed device. Use this command on a managed device to configure the IP address and preshared key or certificate for secure communication with the Mobility Conductor. On the Mobility Conductor, use the `localip` command to configure the IP address and pre-shared key or certificate for a managed device.



The parameters in this command can also be defined using the initial setup wizard when the managed device is first configured. Best practices is to define masterip settings using this wizard. If the IP address of the Mobility Conductor on a managed device is changed the managed device should be rebooted.

If your Mobility Conductor and managed devices use a pre-shared key for authentication, they will create the IPsec tunnel using IKEv1. If your Mobility Conductor and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Parameter	Description
<ipaddr>	IP address of the Mobility Conductor.
ipsec <key>	To establish the IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the Mobility Conductor.
interface	Specify the uplink or VLAN interface on the Mobility Conductor to initiate IKE.
peer-mac-1 <peermac-1>	Specify the peer MAC string. NOTE: The peer device is an x86 server, then configure the MAC address of the management interface of the managed device. However, if the peer device is a hardware platform, you must provide the MAC address of the VLAN interface of the managed device.

Parameter	Description
<code>ipsec-custom-cert</code>	Use a custom-installed certificate on the Mobility Conductor to establish a IPsec tunnel using IKEv2.
<code>master-mac1 <mac1></code>	Specify the MAC address of the certificate on the Mobility Conductor.
<code>master-mac2 <mac2></code>	(Optional) Specify the MAC address of the certificate on the redundant Mobility Conductor.
<code>ca-cert <ca></code>	User-defined name of a trusted CA certificate installed on the Mobility Conductor. Use the <code>show crypto-local pki TrustedCA</code> command to display the CA certificates that have been imported into the Mobility Conductor.
<code>server-cert <cert></code>	User-defined name of a server certificate installed on the Mobility Conductor. Use the <code>show crypto-local pki ServerCert</code> command to display the server certificates that have been imported into the Mobility Conductor.
<code>interface</code>	Specify the uplink or VLAN interface on the Mobility Conductor to initiate IKE.
<code>uplink</code>	Use the Mobility Conductor's current active uplink to initiate IKE.
<code>vlan <id></code>	Specify a VLAN interface on the Mobility Conductor to initiate IKE. If you do not specify a VLAN, the managed device IP will be used.
<code>fqdn <fqdn></code>	Identify a dynamically addressed managed device by entering the FQDN of the managed device.
<code>suite-b</code>	If you configure your Mobility Conductor and managed devices to use IKEv2 and custom-installed certificates, you can optionally use Suite- B cryptographic algorithms for IPsec encryption. Specify one of the following options: <ul style="list-style-type: none"> ▪ <code>gcm-128</code> Use 128-bit AES-GCM Suite-B encryption ▪ <code>gcm-256</code> Use 256-bit AES-GCM Suite-B encryption
<code>ipsec-factory-cert</code>	Use the factory-installed certificate on the Mobility Conductor to establish a master/conductor-local IPsec tunnel using IKEv2.
<code>master-mac1 <mac1></code>	Specify the MAC address of the certificate on the Mobility Conductor.
<code>master-mac2 <mac2></code>	(Optional) The MAC address of the certificate on the backup Mobility Conductor.

Parameter	Description
interface	Specify the uplink or VLAN interface on the Mobility Conductor to initiate IKE.
uplink	Use the Mobility Conductor's current active uplink to initiate IKE.
vlan <id>	Specify a VLAN interface on the Mobility Conductor to initiate IKE. If you do not specify a VLAN, the managed device IP will be used.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the managed device.
suite-b	If you configure your Mobility Conductor and managed devices to use IKEv2 and custom-installed certificates, you can optionally use Suite- B cryptographic algorithms for IPsec encryption. Specify one of the following options: <ul style="list-style-type: none"> gcm-128 Use 128-bit AES-GCM Suite-B encryption gcm-256 Use 256-bit AES-GCM Suite-B encryption
vpn-ip <vpn-ip>	Specify the IP address of the VPN concentrator or the FQDN.
ipsec	Establish a IPsec secure communication between the conductor and the local.
ipsec-custom-cert	Use a custom-installed certificate on the Mobility Conductor to establish a IPsec secure communication between the master/ conductor and the local.
ipsec-factory-cert	Use a factory-installed certificate on the Mobility Conductor to establish a IPsec secure communication between the master/ conductor and the local.
web-socket-acp	Configure web-socket connection with ACP.

Example

The following commands configure the Mobility Conductor with a pre-shared key:

```
(host)[mynode] (config) #masterip/conductorip 10.1.1.250 ipsec gw1234567
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The suite-b gcm-128 and suite-b gcm-256 encryption options for IPsec custom certificates requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Available in the config mode on Mobility Conductor.

masteripv6/conductoripv6

```
masteripv6/conductoripv6 <masteripv6_val>
  ipsec <key> [fqdn <fqdn>][interface uplink|vlan <id>] [masteripv4 <masteripv4_val>] [peer-mac-1 <peermac-1>] [peer-mac-2 <peermac-2>]
  ipsec-custom-cert master-mac-1-c <mac-1-c> [master-mac2 <mac2>] ca-cert <ca>
  server-cert <cert> [interface uplink|{vlan <id>}] [fqdn <fqdn>] [suite-b gcm-128|gcm-256]
  ipsec-factory-cert master-mac-1 <MAC> [master-mac2 <mac2>] [interface uplink|{vlan <id>}] [fqdn <fqdn>]
  vpn-ipv6 <vpnipv6>
```

Description

This command configures the IPv6 address and pre-shared key or certificate for the Mobility Conductor or a managed device. Use this command on a managed device to configure the IP address and pre-shared key or certificate for secure communication with the Mobility Conductor. On the Mobility Conductor, use the `localip` command to configure the IP address and pre-shared key or certificate for a managed device.



ArubaOS reboots the managed device when the primary IPv6 address is changed on the managed device. However, a change in the secondary IPv6 address does not require a reboot of the managed device.

If your Mobility Conductor and managed devices use a pre-shared key for authentication, they will create the IPsec tunnel using IKEv1. If your Mobility Conductor and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Parameter	Description
<ipaddr>	IP address of the Mobility Conductor.
ipsec <key>	To establish the IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the Mobility Conductor. NOTE: FQDN is currently not supported for IPv6 address.
interface	Specify the uplink or VLAN interface on the Mobility Conductor to initiate IKE.
uplink	Use the Mobility Conductor's current active uplink to initiate IKE.

Parameter	Description
<code>vlan <id></code>	Specify a VLAN interface on the Mobility Conductor to initiate IKE. If you do not specify a VLAN, the Mobility Conductor IP will be used.
<code>masteripv4 <masteripv4_val></code>	Configure the corresponding IPv4 address of the Mobility Conductor. NOTE: The configuration of the <code>masteripv4 <masteripv4_val></code> sub-parameter is optional in a native IPv6 deployment.
<code>peer-mac-1 <peermac-1></code>	Specify the peer MAC address on the primary Mobility Conductor.
<code>peer-mac-2 <peermac-2></code>	(Optional) Specify the peer MAC address on the redundant Mobility Conductor.
<code>ipsec-custom-cert</code>	Use a custom-installed certificate on the Mobility Conductor to establish a IPsec tunnel using IKEv2.
<code>master-mac1 <mac1></code>	Specify the MAC address of the certificate on the Mobility Conductor.
<code>master-mac2 <mac2></code>	(Optional) Specify the MAC address of the certificate on the redundant Mobility Conductor.
<code>ca-cert <ca></code>	User-defined name of a trusted CA certificate installed on the Mobility Conductor. Use the <code>show crypto-local pki TrustedCA</code> command to display the CA certificates that have been imported into the Mobility Conductor.
<code>server-cert <cert></code>	User-defined name of a server certificate installed on the Mobility Conductor. Use the <code>show crypto-local pki ServerCert</code> command to display the server certificates that have been imported into the Mobility Conductor.
<code>suite-b</code>	If you configure your master/ conductor and managed devices to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: <ul style="list-style-type: none"> ▪ gcm-128 Use 128-bit AES-GCM Suite-B encryption ▪ gcm-256 Use 256-bit AES-GCM Suite-B encryption
<code>ipsec-factory-cert</code>	Use the factory-installed certificate on the Mobility Conductor to establish a master/ conductor -local IPsec tunnel using IKEv2.
<code>master-mac1 <mac1></code>	Specify the MAC address of the certificate on the Mobility Conductor.

Parameter	Description
master-mac2 <mac2>	(Optional) The MAC address of the certificate on the backup Mobility Conductor.
interface	Specify the uplink or VLAN interface on the Mobility Conductor to initiate IKE.
uplink	Use the Mobility Conductor's current active uplink to initiate IKE.
vlan <id>	Specify a VLAN interface on the Mobility Conductor to initiate IKE. If you do not specify a VLAN, the managed device IP will be used.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the managed device.
vpn-ipv6 <vpnipv6>	IPv6 address of the VPN concentrator to establish IPsec tunnel.

Example

The following command configures the Mobility Conductor with a pre-shared key:

```
(host) [00:0b:86:dd:87:00] (config) #masteripv6/conductoripv6 2001::1 ipsec
Aruba@123 masteripv4 10.20.1.1
```

The following command configures the managed device with an IPsec pre-shared key:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2021:1:1:146::9 ipsec
itsabug peer-mac-1 00:15:5D:14:1F:1C peer-mac-2 00:0C:29:BC:89:9B interface
vlan 147 masteripv4 10.16.146.9
```

The following command configures the managed device with a factory-installed certificate:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2001:77::40 ipsec-
factory-cert master-mac-1 20:4c:03:0e:d2:ec master-mac-2 20:4c:03:0e:d2:84
interface-f vlan-f 79 masteripv4 10.15.77.40
```

The following command configures the managed device with a custom-installed certificate:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2021:1:1:166::254 ipsec-
custom-cert master-mac-1 00:0c:29:42:4c:b6 ca-cert CA server-cert VMC-CERT
interface vlan 164 masteripv4 10.16.166.254
```

The following command configures the branch office controller with a factory-installed certificate:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2021:1:1:146::9 vpn-ipv6
2001:192:192:201::42 ipsec-factory-cert vpn-mac-1 00:0b:86:b5:6b:c7
interface vlan 172 masteripv4 10.16.146.9
```

The following command configures the branch office controller with an IPsec pre-shared key:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2021:1:1:166::254 vpn-
ipv6 2001:192:192:201::3 ipsec itsabug peer-id 20:4C:03:44:13:C8 interface vlan 2000
masteripv4 10.16.166.254
```

The following command configures the branch office controller with a custom-installed certificate:

```
(host) *[mynode] (config) #masteripv6/conductoripv6 2021:1:1:166::254 vpn-
ipv6 2001:192:192:201::11 ipsec-custom-cert vpn-mac-1-c 00:0b:86:b5:6b:c7
ca-cert-v BOC-CA server-cert-v BOC_cert interface vlan 172 masteripv4
10.16.166.254
```

Command History

Release	Modification
ArubaOS 8.6.0.0	The following parameters were added: <ol style="list-style-type: none"> 1. <code>vpn-ipv6 <vpnipv6></code> 2. <code>peer-mac-1 <peermac-1></code> 3. <code>peer-mac-2 <peermac-2></code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The suite-b gcm-128 and suite-b gcm-256 encryption options for IPsec custom certificates requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Available in the config mode on Mobility Conductor.

master-redundancy peer-ip-address/conductor-redundancy peer-ip-address

```
master-redundancy/conductor-redundancy
  peer-ip-address [<ipaddr>|ipv6 <ipv6-addr>]
    ipsec <key>
    ipsec-custom-cert peer-mac <mac> ca-cert <ca> server-cert <sc> [suite-b
    gcm128|gcm256]
    ipsec-factory-cert peer-mac <mac>
```

Description

This command configures the IP address and PSK or certificate for a redundant Mobility Conductor on another Mobility Conductor. Use this command on a Mobility Conductor to configure the IP address and pre-shared key or certificates for communication with a redundant Mobility Conductor. If your Mobility Conductor uses a pre-shared key for authentication, it will create the IPsec tunnel using IKEv1. If your Mobility Conductor and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Parameter	Description
<ipaddr>	The IPv4 address of the redundant Mobility Conductor. Use the 0.0.0.0 address to configure a global preshared key for all inter-controller communications.
ipv6 <ipv6-addr>	The IPv6 address of the redundant Mobility Conductor.
ipsec <key>	To establish the IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
ipsec-custom-cert	Use a custom-installed certificate on the Mobility Conductor to establish the IPsec tunnel using IKEv2.
peer-mac <mac>	The peer MAC address of the certificate on the redundant Mobility Conductor.
ca-cert <ca>	User-defined name of a trusted CA certificate installed on the redundant Mobility Conductor. Use the <code>show crypto-local pki TrustedCA</code> command to display the CA certificates that have been imported into the controller.
server-cert <cert>	User-defined name of a server certificate installed on the redundant controller. Use the <code>show crypto-local pki ServerCert</code> command to display the server certificates that have been imported into the Mobility Conductor.

Parameter	Description
suite-b	If you configure your Mobility Conductor to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: <ul style="list-style-type: none"> ▪ gcm-128 Use 128-bit AES-GCM Suite-B encryption ▪ gcm-256 Use 256-bit AES-GCM Suite-B encryption
ipsec-factory-cert	Use the factory-installed certificate on the Mobility Conductor to establish a master/ conductor -local IPsec tunnel using IKEv2.
peer-mac <mac>	The MAC address of the certificate on the redundant Mobility Conductor.

Example

The following command configures the managed device by using the IPv6 address of the redundant Mobility Conductor:

```
(host) [md] (config) #peer-ip-address ipv6 2001:1:2:2020::1 ipsec-custom-
cert master/conductor-mac 00:02:2D:11:55:4D ca-cert cacert1 server-cert
server1
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The <code>ipv6 <ipv6-addr></code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	The suite-b gcm-128 and suite-b gcm-256 encryption options for IPsec custom certificates requires the Advanced Cryptography license. All other parameters are available in the base operating system.	Config mode on Mobility Conductor.

mdconnect

mdconnect

Description

This command allows a user to log in to a managed device without a username and password after logging in to a Mobility Conductor. Change the configuration node to a managed device and execute this command or **mdc**, its short-version to direct the session to the CLI prompt of the managed device. The keyword **MDC** is shown in the CLI prompt to distinguish the managed device and the Mobility Conductor. On the managed device, a user can issue only show commands. Use the `mdconnect` command to log in to a managed device without a username and password.

Parameter	Description
mdconnect	Log in to a managed device without a username and password.

Example

The following command allows a user to log in to a managed device named **VMC** mapped to a device with MAC address 01:02:03:04:05:06:

```
(host) [mynode] #change-config-node VMC
(MM) [01:02:03:04:05:06] #mdconnect

Redirecting to Managed Device Shell
Last login: Wed Nov 2 08:37:48 2016 from X.X.X.X
(VMC) [MDC] #exit

Exiting Managed Device Shell
(MM) [01:02:03:04:05:06] (config) #

The following command allows a user to log in to a managed device with MAC
address 0a:0b:0c:0d:0e:0f:
(host) [mynode] #change-config-node /md/0a:0b:0c:0d:0e:0f
(MM) [0a:0b:0c:0d:0e:0f] #mdconnect

Redirecting to Managed Device Shell
Last login: Wed Nov 2 08:38:48 2016 from X.X.X.X
(test) [MDC] #exit

Exiting Managed Device Shell
(MM) [0a:0b:0c:0d:0e:0f] (config) #
```

Related Commands

Command	Description
change-config-node	Displays the configuration node hierarchy.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

mesh-recovery-generate

```
mesh-recovery-generate
  {license <license> | serial <serial> mac <mac> }
  override
  unencrypted
```

Description

This command is used to generate a mesh recovery profile.

Parameter	Description
license <license>	Specify a license string or a 48 characters long string.
override	Override current recovery profile with the generated one. NOTE: Do 'write mem' to store the generated profile in the configuration file.
unencrypted	Display unencrypted wpa-hexkey (for debugging).
serial <serial>	Specify serial number of the controller.
mac <mac>	Specify MAC address of the controller.
override	Override current recovery profile with the generated one.

Parameter	Description
	NOTE: Do 'write mem' to store the generated profile in the configuration file.
unencrypted	Display unencrypted wpa-hexkey (for debugging).

Example

```
(host) [mynode] (config) #mesh-recovery-generate license default
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	enable mode on Mobility Conductor.

mgmt-server

```
mgmt-server
  primary-server <primary-server-ip> profile <profile-name> [secure] [transport
  {mix|udp|websocket}]
  profile <profile-name>
    airgroupinfo-enable
    ap-app-stats
    ap-stats
    clone <source>
    generic-amon-enable
    inline-ap-stats
    inline-auth-stats
    inline-ctrl-assoc-stats
    inline-dhcp-stats
    inline-dns-stats
    inline-lldp-stats
    location-enable
    misc-enable
    monitored-info-del-enable
    monitored-info-enable
    monitored-info-snapshot-enable
    no
    sessions-enable
    stats-enable
    stats-extended-enable
    tag-enable
    uccmonitoring-enable
    user-visibility-enable
    wan-state
    wids-event-info-enable
  source-ipv6-address
```

Description

This command configures the management server profile. Register a management server with the Mobility Conductor by specifying the IP address of an AirWave management server or ALE that should receive messages from the Mobility Conductor using the AMON protocol. You must also specify the management configuration profile in which the AMON message filtering settings can be done. The default profiles provided for the AirWave server (default-amp) and ALE (default-ale) are editable using this command.

The IDS WLAN management system (WMS) on the managed device monitors wireless traffic to detect any new AP or wireless client station that tries to connect to the network. ArubaOS can send Clarity Live and user serviceability statistics from a managed device to a management server, which can use this data to identify the client connectivity issues.

A managed device can also collect information about each step in the user authentication process, and send these records to a management server in the AMON format, the data transport

protocol used to communicate basic statistics or state changes to the management servers such as AirWave or ALE.

Parameter	Description
primary-server <primary-server-ip> profile <profile-name> [secure transport]	Associate the Mobility Conductor to ALE server or an AirWave management server by entering the IPv4 or IPv6 address of the server and specifying a management configuration profile.
secure	Enabling this specifies that DTLS mode is used.
transport	This defines the type of transport mechanism.
profile	Configure a new management server profile on the Mobility Conductor or to edit the default profiles.
airgroupinfo-enable	If enabled, the messages related to the AirGroup feature will be sent to the management server.
ap-app-stats	Enables reporting client application usage.
app-stats	Enables AP statistics.
clone <source>	Copy from another management configuration profile.
generic-amon-enable	Enables Always On Amon messages.
inline-ap-stats	Enable Clarity Live statistics from the AP.
inline-auth-stats	Enable Clarity Live statistics related to authentication.
inline-ctrl-assoc-stats	Generates the passive controller station AMON messages. The passive controller station AMON messages are not generated by default. To generate the messages, issue the mgmt-server profile <name of the profile> inline-ctrl-assoc-stats command on managed device.
inline-dhcp-stats	Enable Clarity Live statistics of DHCP.
inline-dns-stats	Enable Clarity Live statistics of DNS.
inline-lldp-stats	Enable Clarity Live statistics of LLDP.
location-enable	If enabled, Station RSSI or AP Neighbor messages will be sent to the management server.
misc-enable	If enabled, the AP system statistics, specifications, and station steer information will be sent to the management server.

Parameter	Description
<code>monitored-info-del-enable</code>	Information is sent when a monitored AP or client is deleted.
<code>monitored-info-enable</code>	If enabled, the monitored AP or station information will be sent to the management server.
<code>monitored-info-snapshot-enable</code>	If enabled, the managed device sends a periodic snapshot about the state (up or down) of each monitored AP, client, rogue AP, or suspected rogue AP.
<code>no</code>	Negates or removes a parameter.
<code>sessions-enable</code>	If enabled, the firewall DNA, application, and aggregate session messages will be sent to the management server.
<code>stats-enable</code>	If enabled, the statistics for AP radios, virtual APs, and clients are be sent to the management server.
<code>stats-extended-enable</code>	If enabled, the extended statistics for AP radios, virtual APs, and clients are be sent to the management server.
<code>tag-enable</code>	If enabled, tag messages will be sent to the management server.
<code>uccmonitoring-enable</code>	If enabled, the messages about the unified communications manager are be sent to the management server.
<code>user-visibility-enable</code>	If enabled, the user visibility message are be sent to the management server.
<code>wan-state</code>	If enabled, the WAN state information is to be sent to the management server.
<code>wids-event-info-enable</code>	If enabled, the controller sends messages about current IDS events as soon as they are detected.
<code>source-ipv6-address <src-ipv6-addr></code>	Configure the source IPv6 Address for AMON packets.

Example

The following command defines a primary AirWave Management server.

```
(host) [mynode] (config) #mgmt-server primary-server 192.0.2.10 profile
default-amp
```

Related Commands

Command	Description
ids management-profile	Manage the events correlation for IDS event traps and syslogs (logs).
ids wms-local-system-profile	This command configures the WLAN management system (WMS) service to terminate on individual managed devices instead of Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.17 and 8.7.1.9	The <code>inline-ctrl-assoc-stats</code> parameter was introduced.
ArubaOS 8.7.0.0	The <code>ap-app-stats</code> parameter was introduced.
ArubaOS 8.1.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The <code>primary-server</code> parameter was modified to accept IPv6 address. ■ The Clarity Live parameters such as <code>inline-ap-stats</code>, <code>inline-auth-stats</code>, <code>inline-dhcp-stats</code>, and <code>inline-dns-stats</code> were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mgmt-user

```
mgmt-user
  audit-period
  console-blocks
  localauth <username>
  ssh-pubkey
    client-cert <certname> <username>
    <role> [<rcp>]
  webui-cacert <certificate_name> [serial <number>] <username> <role> [<rcp>]
  <username> <rolename> <max-concurrent-session> [node <path>] <password> <old-
  password>
```

Description

This command configures an administrative user. You can configure client certificate authentication of WebUI or SSH management users (by default, only username/password is used). To configure certificate authentication for the WebUI or SSH, use the web-server mgmt-auth certificate or ssh mgmt-auth public-key commands, respectively.

- Use `webui-cacert <certificate name>` command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated.
- Use the `mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>` if you want the authentication process to use previously configured certificate name and serial number to derive the user role.
- Use the `mgmt-user webui-cacert <certificate_name> serial <number> <username> <role> <rcp>` command if you want to configure an optional RCP for an ssh-pubkey user.
- Use the `mgmt-user <username> <rolename> node <path> <password>` to configure an authenticated user assigned to a role in the managed device.

Parameter	Description
<code>audit-period</code>	Configures an audit period.
<code>console-blocks</code>	Blocks serial console access once the user logs out.
<code>localauth <username></code>	Enables the authentication of management users based on the results returned by the authentication server. To disable this setting, use the <code>no mgmt-user localauth</code> command. To verify if authentication of local management user accounts is enabled or disabled, use the following command: <code>show mgmt-user local-authentication-mode</code>

Parameter	Description
ssh-pubkey	Configures certificate authentication of administrative users using the CLI through SSH.
client-cert	Displays the name of the X.509 client certificate for authenticating administrative users using SSH.
<username>	Displays the name of the user.
<role>	Displays the role assigned to the authenticated user.
<rcp>	Revocation Checkpoint for the ssh user's client certificate. The rcp checks the revocation status of the SSH user's client certificate before permitting access.
webui-cacert	The client certificate for authenticating administrative users using the WebUI.
<certificate_name>	Displays the name of the CA certificate. If configured, certificate authentication and authorization are automatically completed using an authentication server.
serial	Displays the serial number of the client certificate.
<username>	Displays the name of the user.
<role>	Displays the role assigned to the authenticated user.
<rcp>	Revocation Checkpoint for the ssh user's client certificate. The rcp checks the revocation status of the SSH user's client certificate before permitting access.
<username>	<p>Displays the name of the user.</p> <p>You can create a maximum of 10 management users. Starting from ArubaOS 8.10.0.0, the username can have a maximum of 128 characters.</p> <p>NOTE: If you configure a root management user, you can use special characters except for double-byte characters.</p>
<rolename>	<p>Role assigned to the user. Predefined roles include:</p> <ul style="list-style-type: none"> ▪ guest-provisioning: Allows the user to create guest accounts on a special WebUI page. ▪ location-api-mgmt: Permits access to location API information. You can log into the CLI; however, you cannot use any CLI commands. ▪ network-operations: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log into the CLI; however, you can only use a subset of CLI commands to monitor the controller.

Parameter	Description
	<ul style="list-style-type: none"> read-only: Permits access to CLI show commands or WebUI monitoring pages only. root: Permits access to all management functions on the controller. standard: This role has root privileges but cannot make changes to the management users.
max-concurrent-sessions	Configures the maximum concurrent session for a management user. The maximum number of sessions allowed are 10.
node	Configures node level permissions. Use this parameter when you want to configure an authenticated user assigned to a role in the managed device.
<path>	Path of the managed device.
<password>	<p>NOTE: You are prompted for the <password> for this user after you type in <role> and press Enter.</p> <p>The password must have a minimum of six characters. Starting from ArubaOS 8.10.0.0, the password can have a maximum of 128 characters. Starting from ArubaOS 8.10.0.0, the password can have a maximum of 128 characters. You can use special characters in the management user password. The restrictions are as follows:</p> <ul style="list-style-type: none"> You cannot use double-byte characters You cannot use the question mark (?) You cannot use white space <space >
<old-password>	Provides the old password, to enable the user to change the management user password.

Example

The following command configures a management user and role:

```
(host)[node](config) #mgmt-user testuser1 root
Password: *****
Re-Type password: *****
```

Related Commands

Version	Modification
show mgmt-user	Displays a list of management users on the Mobility Conductor and details of each management user.

Command History

Release	Modification
ArubaOS 8.10.0.0	The username and password can have a maximum of 128 characters.
ArubaOS 8.4.0.0	The following sub-parameters were introduced in the <code><username></code> parameter: <ul style="list-style-type: none"> ▪ <code>max-concurrent-sessions</code> ▪ <code>old-password</code> The <code>audit-period</code> parameter was introduced.
ArubaOS 8.2.2.0	The following sub-parameters were introduced in the <code><username></code> parameter: <ul style="list-style-type: none"> ▪ <code>max-concurrent-sessions</code> ▪ <code>old-password</code> The <code>audit-period</code> parameter was introduced.
ArubaOS 8.1.0.0	The <code>standard</code> role was introduced.
ArubaOS 8.0.1.0	The <code>node</code> parameter was introduced in the <code>mgmt-user <username> <rolename></code> command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mobility-manager

```
mobility-manager <A.B.C.D>  
  user <word> <string>  
    auth-prot {md5 | sha} <string>  
      priv-prot {AES | DES} <string>  
    interval <secs>  
    retrycount <count>  
    rtls <rtls-portnumber>  
    trap-version {1 | 2c | 3}  
    udp-port <portnumber>
```

Description

Use the command to allow a managed device to communicate with a mobility manager server (MMS). To configure a username and password for the managed device to communicate with MMS, execute the following command:

```
(host) [mm] (config) #mobility-manager 1.1.1.1 user testUN1 testUN1
```

The interval time, retry count, RTLS port number, and UDP port number are optional parameters that can be configured using the `mobility-manager` command.

If you try to configure a third mobility manager server, the following message is displayed:
Maximum number of 2 MMS servers already configured.

Parameter	Description
<A.B.C.D>	Configures the IP address of the mobility manager server for the managed device to communicate with.
user <word> <string>	Configures the username and password to communicate with MMS. Username: string of length 1-31, Password: string of length 1-31
auth-prot {md5 sha} <string>	Configures authentication protocol of the user with password. <ul style="list-style-type: none">■ md5: HMAC-MD5-96 Digest Authentication Protocol■ sha: HMAC-SHA-96 Digest Authentication Protocol■ <string> : Authentication Password 8-31 bytes
priv-prot {AES DES} <string>	Configures the privacy protocol of the user with password. <ul style="list-style-type: none">■ AES: CFB128-AES-128 Symmetric Encryption Protocol■ DES: CBC-DES Symmetric Encryption

Parameter	Description
	Protocol <ul style="list-style-type: none"> ■ <string> : Authentication Password 8-31 bytes
interval <secs>	Configures the time it takes for a UDP packet to travel to and from the trap server (round-trip time). This value indicates the timeout. 0-65535
retrycount <count>	Configures the maximum number of retries allowed to authenticate with MMS. 0-256
rtls <rtls-portnumber>	Configures the UDP port number for RTLS data collection. string of length 1-256 8000
trap-version {1 2c 3}	Configures trap server's SNMP version. 1, 2c, or 3
udp-port <portnumber>	Configures trap server's UDP port number. 1-65535 162

Example

The following command is an example to configure MMS and allow a managed device to communicate with it:

```
(host) [mm] (config) #mobility-manager 1.1.1.1 user testUN1 testUN1 auth-prot md5 authpswd interval 250
```

Related Commands

Command	Description
show mobility-managers	This command displays information of MMS.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mon-serv-debug

```
mon-serv-debug {enable | disable}
  all-devices key-mac <dev-key>
  ap key-mac <dev-key>
  mesh key-mac <dev-key>
  radio key-mac <dev-key>
  sta key-mac <dev-key>
  vap key-mac <dev-key>
  wan key-mac <dev-key>
```

Description

This command is used to enable or disable debug logs.

Parameter	Description
enable	Enable debugging.
disable	Disable debugging.
all-devices	Debugging of all device logs.
ap	Debugging of AP device logs.
mesh	Debugging of mesh AP device logs.
radio	Debugging of radio device logs.
sta	Debugging of station device logs.
vap	Debugging of VAP device logs.
wan	Debugging of WAN dashboard related device logs.
key-mac <dev-key>	Specify MAC address of the device.

Example

The example below enables debugging for the AP with MAC address 11.22.33.44.55.66.

```
(host) [mynode] (config) ##mon-serv-debug enable ap key-mac
11.22.33.44.55.66
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mon-serv-fwv-toggle-amon-traffic-filter

mon-serv-fwv-toggle-amon-traffic-filter

Description

Toggle AMON traffic filter.

Example

The example below enables AMON traffic filter.

```
(host) [mynode] (config) #mon-serv-fwv-toggle-amon-traffic-filter
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mon-serv-mon-log

```
mon-serv-mon-log {enable | disable}
```

Description

Enable mon-serv MON debug logs.

Example

The example below enables mon-serv MON debug logs.

```
(host) [mynode] (config) #mon-serv-mon-log
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mon-serv-set-gap-read-timer

```
mon-serv-set-gap-read-timer <key>
```

Description

Set GAP read timer in minutes. To disable periodic sync, set the key value to 0.

Parameter	Description
<key>	Set the GAP read timer value in minutes

Example

The example below sets GAP read timer value to 5 minutes.

```
(host) [mynode] (config) #mon-serv-set-gap-read-timer 5
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

mon-serv-toggle-amon-traffic-filter

```
[no] mon-serv-toggle-amon-traffic-filter
```

Description

Enable AMON traffic filter. Issue the `no mon-serv-toggle-amon-traffic-filter` command to disable AMON UDP and re-enable it again using the command `mon-serv-toggle-amon-traffic-filter`.

Example

The example below enables AMON traffic filter.

```
(host) [mynode] (config) #mon-serv-toggle-amon-traffic-filter
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

netdestination

```
netdestination <dstname>
  description <description6>
  host <ipaddr> {vlan <vlanID> | offset <offset No>}
  invert
  name <host_name>
  network <ipaddr> <netmask>
  no ...
  range <start-ipaddr> <end-ipaddr>
```

Description

This command configures an alias for an IPv4 network host, subnetwork, or range of addresses. Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination in multiple session ACLs. Once you configure an alias, you can use it to manage network and host destinations from a central configuration point, because all policies that reference the alias will be updated automatically when you change the alias.

To create a local net destination override, use the **host vlan offset** option.

For example:

```
netdestination store
host vlan 10 offset 5
host vlan 10 offset 8
```

The subnets to a particular VLAN can be assigned by the bulk edit tool. With the above, user can pick whatever the subnet (for example 10.1.1.0/24) assigned to vlan 10 for that store and calculate offsets 5 (10.1.1.5) and 8 (10.1.1.8) from it.

When using the **invert** option, use caution when defining multiple aliases, as entries are processed one at a time. As an example, consider a netdestination configured with the following two network hosts:

```
netdestination dest1
invert
network 1.0.0.0 255.0.0.0
network 2.0.0.0 255.0.0.0
```

A frame from http://1.0.0.1 would match the first alias entry, (which allows everything except for 1.0.0.0/8) so the frame would be rejected. However, it would then be compared against the second alias, which allows everything except for 2.0.0.0/8, and the frame would be permitted.

Parameter	Description
<dstname>	Name for this host or domain. Maximum length is 63 characters.
description	Description about the this destination up to 128 characters long.

Parameter	Description
host	Configures a single IPv4 host.
A.B.C.D	Specify IPv4 address of the host.
vlan <1-4094>	Specify IPv4 address based on VLAN.
offset <1-254>	Specify offset in the VLAN subnet.
invert	Specifies that the inverse of the network addresses configured are used. For example, if a network of 172.16.0.0 255.255.0.0 is configured, this parameter specifies that the alias matches everything except this subnetwork.
name	<p>Use the <code>name</code> parameter to specify a domain or host name inside the <code>netdestination</code> object. Wildcards are supported through the asterisk (*) symbol, with the limitations described in the examples below.</p> <ul style="list-style-type: none"> ■ A wildcard '*' is allowed only once and only in the beginning of the host or domain name. (For instance, *.example.com is allowed, but example*.com and *example*.com are not allowed.) ■ If the wildcard is applied to the host, the <code>netdestination</code> matches all hosts ending with that specific domain. (The name *.example.com matches all hosts ending with the domain .example.com, such as demo.example.com.) ■ If the wildcard is applied to the domain, the <code>netdestination</code> matches all hosts ending with that domain string. (The name *example.com matches all domains ending with example.com, such as myexample.com and domainexample.com.)
network	An IPv4 subnetwork consisting of an IP address and netmask.
no	Negates any configured parameter.
range	A range of IPv4 addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a subnetwork and use the <code>network</code> parameter.

Example

The following command configures an alias for an internal network:

```
(host)[node](config) #netdestination Internal
(host)[node](config-dest) #network 10.1.0.0 255.255.0.0
```

The following command overrides the local network destination:

```
(host)[node](config)#netdestination store
(host)[node](config-dest)#host vlan 55 offset 36
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

netdestination6

```
netdestination6 <dstname>
  description <description6>
  host <ipaddr>
  invert
  name <host_name>
  network <ipaddr> <netmask>
  no ...
  range <start-ipaddr> <end-ipaddr>
```

Description

This command configures an alias for an IPv6 network host, subnetwork, or range of addresses. Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination. Once you configure an alias, you can use it in multiple session ACLs.

When using the **invert** option, use caution when defining multiple aliases, as entries are processed one at a time. As an example, consider a netdestination configured with the following two network hosts:

```
netdestination6 dest1 invert
network 2002:0:0:0:0:0:100:0/128
network 2002:0:0:0:0:0:200:0/128
```

A frame from http://1.0.0.1 would match the first alias entry, (which allows everything except for 2002:0:0:0:0:0:100:0/128) so the frame would be rejected. However, it would then be compared against the second alias, which allows everything except for 2002:0:0:0:0:0:200:0/128, and the frame would be permitted.

Parameter	Description
<dstname>	Name of the IPv6 destination host or subnetwork up to 63 characters long.
description	Description about the IPv6 netdestination up to 128 characters long.
host	Configures a single IPv6 host.
invert	Specifies that the inverse of the network addresses configured are used. For example, if a network of fe80:0:0:0:0:0:ac10:0/128 is configured, this parameter specifies that the alias matches everything except this subnetwork.
name	Use the <code>name</code> parameter to specify a domain or host name inside the netdestination object. Wildcards are supported through the asterisk (*) symbol, with the limitations described in the examples below.

Parameter	Description
	<ul style="list-style-type: none"> ■ A wildcard '*' is allowed only once and only in the beginning of the host or domain name. (For instance, *.example.com is allowed, but example*.com and *example*.com are not allowed). ■ If the wildcard is applied to the host, the netdestination matches all hosts ending with that specific domain. (The name *.example.com matches all hosts ending with the domain .example.com, such as demo.example.com). ■ If the wildcard is applied to the domain, the netdestination matches all hosts ending with that domain string. (The name *example.com matches all domains ending with example.com, such as myexample.com and domainexample.com).
network	An IPv6 subnetwork consisting of an IP address and netmask.
no	Negates any configured parameter.
range	A range of IPv6 addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a sub-network and use the <code>network</code> parameter.

Example

The following command configures an alias for an internal network:

```
(host) [mynode] (config) #netdestination6 Internal
(host) [mynode] (config-submode) #network fe80:0:0:0:0:a01:0/128
```

The following example displays the use of extended scope of address range:

```
(host) [mynode] (config) #netdestination6 ipv6-reserved-range
(host) [mynode] (config-submode) #invert
(host) [mynode] (config-submode) #network 2000::/3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

netexthdr

```
netexthdr <name>  
  eh <eh-type> deny | permit
```

Description

This command allows you to edit the packet filter options in the extension header (EH). ArubaOS firewall is enhanced to process the IPv6 extension header (EH) to enable IPv6 packet filtering. You can filter the incoming IPv6 packets based on the EH type. You can edit the packet filter options in the default EH, using this command. By default, the default EH alias permits all EH types.

Parameter	Description
<name>	Specify the EH alias name.
eh <eh-type>	Specify one of the following EH types: <ul style="list-style-type: none">▪ <0-255>: Matches the IPv6 next header type▪ authentication: Matches the IPv6 authentication header▪ dest-option: Matches the IPv6 destination-option header▪ esp: Matches the IPv6 encapsulation security payload header▪ fragment: Matches the IPv6 fragment header▪ hop-by-hop: Matches the IPv6 hop-by-hop header▪ mobility: Matches the IPv6 mobility header▪ routing: Matches the IPv6 routing header
deny	Denies the IPv6 packets matching the specified extended header type.
permit	Permits the IPv6 packets matching the specified extended header type. NOTE: By default, all the EH types are supported in the default EH.

Example

The following command denies the IPv6 packets matching the specified extended header type in the default EH:

```
(host) [node] (config) #netexthdr default  
(host) [node] (config-exthdr) #eh authentication deny
```

Related Commands

Command	Description
<code>show netexthdr</code>	Displays the IPv6 extension header (EH) types that are denied.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

net service

```
net service <name> <protocol>|tcp|udp {list <port>,<port>}|<port> [<port>]}  
[ALG <service> | http-proxy | https-proxy]
```

Description

This command configures an alias for network protocols. Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the network service. Once you configure an alias, you can use it in multiple session ACLs.

Parameter	Description
net service	Name for this alias.
<protocol>	IP protocol number. 0-255
tcp	Configure an alias for a TCP protocol
udp	Configure an alias for a UDP protocol
list <port>,<port>	Specify a list of non-contiguous port numbers, by entering up to six port numbers, separated by commas. 0-65535
<port> [<port>]	TCP or UDP port number. You can specify a single port number, or define a port range by specifying both the lower and upper port numbers. 0-65535
ALG	Application-level gateway (ALG) for this alias.
<service>	Specify one of the following service types: <ul style="list-style-type: none">▪ dhcp: Service is DHCP▪ dns: Service is DNS▪ facetime: Service is Facetime▪ ftp: Service is FTP▪ h323: Service is H323▪ jabber: Service for Jabber▪ noe: Service is Alcatel NOE▪ rtsp: Service is RTSP▪ sccp: Service is SCCP▪ sip: Service is SIP▪ sips: Service is Secure SIP▪ svp: Service is SVP▪ tftp: Service is TFTP

Parameter	Description
	<ul style="list-style-type: none"> ▪ vocera: Service is VOCERA
http-proxy	HTTP proxy port.
https-proxy	HTTPS proxy port.

Example

The following command configures an alias for a network service:

```
(host)[mynode](config) #netSERVICE HTTP tcp 80
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

no allowed-address-list

```
no allowed-address-list
  ipv4
  ipv6
```

Description

This command is used to remove the IP addresses that were added using `allowed-address-list` command.

Parameter	Description
ipv4	This parameter deletes the IPv4 addresses from the allowed address list.
ipv6	This parameter deletes the IPv6 addresses from the allowed address list.

Example

```
(host) [mynode] #no allowed-address-table ipv4 10.12.133.15
```

Related Commands

Command	Description
<code>allowed-address-list</code>	Configures addresses exempted when the deny-inter-user-bridging is enabled.
<code>show allowed-address-list</code>	Displays the list of allowed addresses that are exempted.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and managed device.

no packet-capture

```
no packet-capture  
  controlpath  
  datapath  
  destination
```

Description

This command disables packet capturing for debugging.

Parameter	Description
<pre>controlpath {interprocess {all <ports>} other sysmsg {all <opcodes>} tcp {all <ports>} udp {all <ports>}}</pre>	<p>Disables capturing following interprocess packets on control path:</p> <ul style="list-style-type: none">▪ interprocess {all <ports>}: Disables capturing packets on all or up to 10 comma separated ports.▪ other: Disables capturing other types of packets.▪ sysmsg {all <opcodes>}: Disables capturing internal messaging packets on all or up to 10 comma separated ports.▪ tcp {all <ports>}: Disables capturing TCP packets on all or up to 10 comma separated ports.▪ udp {all <ports>}: Disables capturing UDP packets on all or up to 10 comma separated ports.
<pre>datapath {ipsec {all-v4 all-v6 <peer-ip> <peer-ipv6>} wifi-client <mac-address> {all decrypted encrypted}}</pre>	<p>Disables capturing following packets on datapath:</p> <ul style="list-style-type: none">▪ ipsec {all-v4 all-v6 <peer-ip> <peer-ipv6>}: Disables capturing all IPsec packets from given peer (inner IPv4), all IPsec packets from given peer (inner IPv6), given peer (IPv4), or given peer (IPv6) address.▪ wifi-client <mac-address> {all decrypted encrypted}: Disables capturing all IPsec packets, decrypted IPsec packets, or encrypted packets from given MAC address.
<pre>destination {interface <slot/port> ip-address <ipaddr> local-filesystem}</pre>	<p>Disables capturing following packets on destination:</p> <ul style="list-style-type: none">▪ interface <slot/port>: Stops sending captured packets to the slot/port of an

Parameter	Description
	<p>interface.</p> <ul style="list-style-type: none"> ▪ ip-address <ipaddr>: Stops sending captured packets to the given IP address of a remote destination. ▪ local-filesystem: Stops sending captured packets in pcap files.

Example

Access the CLI and use the following command to disable other packet-capture:

```
(host) [mynode] #no packet-capture controlpath other
```

Access the CLI and use the following command to disable all packet-capture from a wifi-client:

```
(host) [md] #no packet-capture datapath wifi-client 00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

ntp

```
ntp
  authenticate
  authentication-key <keyid> {md5|sha1} <keyvalue>
  debug
  server {<ip>|<ip6>|<fqdn>} {[iburst|key] <keyid>}
  server-mode
  source
  standalone
  trusted-key
```

Description

This command allows you to configure NTP options. Network Time Protocol (NTP) authentication enables the controller to authenticate the NTP server before synchronizing local time with server. This helps identify secure servers from fraudulent servers. This command has to be enabled for NTP authentication to work.

Starting from 8.1.0.0, you can specify the source address for NTP traffic originating from the Mobility Conductor using the `source` parameter. Before this enhancement, the NTP traffic's source address was dynamically decided by the **NTP** module. The source of the NTP client traffic can be either a loopback interface or a specific VLAN ID. To allow time synchronization to be independent of any physical interfaces that could be down, use the loop back interface as the NTP source address.

Syntax

Parameter	Description
<code>authenticate</code>	This parameter enables the controller to authenticate the NTP server before synchronizing local time with server. This helps identify secure servers from fraudulent servers. This command has to be enabled for NTP authentication to work.
<code>authentication-key</code>	This command configures a key identifier and secret key and adds them into the database. NTP authentication works with a symmetric key configured by user. The key is shared by the client (Aruba managed device) and an external NTP server.
<code><key-id></code>	The key identifier is a string that is shared by the client (Arubamanaged device) and an external NTP server. This value is added into the database.
<code>md5 sha1 <keyvalue></code>	The key value is a secret string, which along with the key identifier, is used for authentication. This is added into the database.

Parameter	Description
debug	Enable NTP debug.
server	This command configures an NTP server. You can configure the Mobility Conductor to set its system clock using NTP by specifying one or more NTP servers.
<ip>/<ip6>/<fqdn>	IPv4/IPv6/FQDN address of the peer.
iburst	(Optional) This parameter causes the Mobility Conductor to send up to ten queries within the first minute to the NTP server. This option is considered "aggressive" by some public NTP servers. disabled
key <key-id>	This is the key identifier used to authenticate the NTP server. This needs to match the key identifier configured in the <code>ntp authentication-key</code> command.
server-mode [disable]	This command disables NTP server mode.
source	This command specifies the source address for NTP client traffic.
loopback	This parameter sets loopback interface as the source for NTP client traffic.
<vlanid>	This parameter sets source VLAN for NTP client traffic.
standalone	This command configures NTP time serve.
vlan-range <word>	Configures VLAN interfaces on which NTP adheres for serving time where: <word>: Represents VLAN range.
trusted-key	This command configures an additional subset of trusted keys which can be used for NTP authentication.
<keyid>	An additional trusted string that can be used for authentication.

Example

The following command configures an NTP server:

```
(host) [mynode] (config) #ntp authenticate
```


The following command configures the loopback interface as the source for NTP client traffic:

```
(host) [mynode] (config) #ntp source loopback
```

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>fqdn</code> sub-parameter was added.
ArubaOS 8.2.0.0	The <code>sha1</code> sub-parameter was added.
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>server-mode</code>■ <code>source</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

ntp authentication-key

```
ntp authentication-key <key-id>
  md5
  sha1
  <keyvalue>
```

Description

This command configures a key identifier and secret key and adds them into the database. NTP authentication works with a symmetric key configured by user. The key is shared by the client (Aruba controller) and an external NTP server.

NTP authentication works with a symmetric key configured by user. The key is shared by the client (Arubacontroller) and an external NTP server. This command adds both the key identifier and secret string into the database.

Parameter	Description	Range	Default
<key-id>	The key identifier is a string that is shared by the client (Aruba controller) and an external NTP server. This value is added into the database.	1-65534	—
md5 sha1	The hash algorithm type—use either md5 or sha1.	—	—
<keyvalue>	The key value is a secret string, which along with the key identifier, is used for authentication. This is added into the database.	0-255 ASCII characters	—

Example

The following command configures the NTP authentication key. For the MD5 hash algorithm, the key identifier is 12345 and the shared secret is 67890.

```
(host) [mynode] (config) #ntp authentication-key 12345 md5 67890
```

The following example shows NTP authentication key configuration using SHA1 hash algorithm:

```
(host) [mynode] (config) #ntp authentication-key 41 sha1 secretkey
```

Command History

Release	Modification
ArubaOS 8.2.1.0	The <code>sha1</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor or Managed Device.

openflow-controller

```
openflow-controller
  auxiliary-channel-port <port>
  host-ageout-time <value>
  mode passive
  no
  openflow-controller-enable
  port <port>
  tls-ca-cert-file <tls-ca-cert-file>
  tls-certificate-file <tls-certificate-file>
  tls-enable
  tls-key-file <tls-key-file>
  topology-discovery-enable
```

Description

This command configures OpenFlow controller on Mobility Conductor. The OpenFlow controller must be configured from the **/mm** node hierarchy of Mobility Conductor. OpenFlow controller is disabled by default. For OpenFlow to be functional in a network, you must enable OpenFlow controller on the Mobility Conductor and OpenFlow agent on the required managed devices. By default, OpenFlow is disabled on Mobility Conductor as well as the managed devices.

Parameter	Description
auxiliary-channel-port	Configures a listening port for OpenFlow controller in the auxiliary channel (UDP) to send and receive packets without consuming bandwidth on the main channel.
host-ageout-time	Configures the ageout time for the host.
mode {passive}	Sets the OpenFlow controller mode. This release of ArubaOS provides support only for passive mode. passive passive
no	Negates any configuration.
openflow-controller-enable	Enables or disables OpenFlow controller on Mobility Conductor disabled
port	The listening port for the OpenFlow controller. 1-65535 6633

Parameter	Description
tls-ca-cert-file	Configures the CA certificate file from the specified path.
tls-certificate-file	Configures the certificate file from the specified path.
tls-enable	Enables or disables TLS. disabled
tls-key-file	Configures the key from the specified path
topology-discovery-enable	Enables the Openflow controller topology. disabled

Examples

The following commands enables OpenFlow controller on Mobility Conductor:

```
(host) [mm] (config) #openflow-controller
(host) [mm] (openflow-controller) #openflow-controller-enable
```

Related Commands

Command	Description
show openflow-controller	Displays the OpenFlow configuration and flow information on Mobility Conductor.
openflow-profile	This command configures OpenFlow profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license.	Config mode on Mobility Conductor.

openflow-profile

```
openflow-profile
  auxiliary-channel-port <port>
  bind-vlan [add|remove] <vlan>
  controller-ip <ip-addr> <port>
  custom-cert-enable
  mode passive
  no
  openflow-auxiliary-enable
  openflow-enable
  tls-ca-cert-file <tls-ca-cert-file>
  tls-certificate-file <tls-certificate-file>
  tls-enable
  tls-key-file <tls-key-file>
  version {v1.0|v1.3}
```

Description

This command configures OpenFlow profile on the managed device. The OpenFlow profile must be configured from the **/md** node hierarchy of Mobility Conductor. OpenFlow profile is disabled by default. For OpenFlow to be functional in a network, you must enable OpenFlow controller on the Mobility Conductor and OpenFlow agent on the required managed devices. By default, OpenFlow is disabled on Mobility Conductor as well as the managed devices.

Parameter	Description
auxiliary-channel-port <port>	Configures a listening port for OpenFlow Controller in the auxiliary channel (UDP) to send and receive packets without consuming bandwidth on the main channel.
bind-vlan [add remove] <vlan>	Configures a specified range of OpenFlow VLANs. You can optionally add or remove the specified VLANs or VLAN range from the configured list of VLANs.
controller-ip <port>	Configures the IP and listening port of the OpenFlow Controller running on Mobility Conductor. 1-65535 6633
custom-cert-enable	Enable or disable non-TPM custom certificate. Disabled
mode {passive}	Sets the OpenFlow agent mode.

Parameter	Description
	This release of ArubaOS provides support only for passive mode. passive passive
no	Negates any configuration.
openflow-auxiliary-enable	Enables or disables OpenFlow auxiliary channel. disabled
openflow-enable	Enables or disables OpenFlow agent on the managed device. disabled
tls-ca-cert-file <tls-ca-cert-file>	Configures the CA certificate file from the specified path.
tls-certificate-file <tls-certificate-file>	Configures the certificate file from the specified path.
tls-enable	Enables or disables TLS. disabled
tls-key-file <tls-key-file>	Configures the key from the specified path
version {v1.0 v1.3}	Configures the OpenFlow version. v1.3

Examples

Execute the following commands to configure and enable the OpenFlow profile:

```
(host) [md] (config) #openflow-profile
(host) [md] (Openflow-profile) #openflow-enable
(host) [md] (Openflow-profile) #controller-ip <master/ conductor -ip> <port>
```

Related Commands

Command	Description
show openflow-profile	Displays the OpenFlow profile configuration information on the managed device.

Command	Description
show openflow	Displays the OpenFlow information on the managed device.
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license.	Config mode on Mobility Conductor.

packet-capture

```
packet-capture
  controlpath
  copy-to-flash {controlpath-pcap | datapath-pcap}
  datapath {ipsec <peer-ip>|<peer-ipv6>} [wifi-client <mac-address> {decrypted |
  encrypted | all}]
  destination [interface <slot/module/port>] [ip-address <ip-address>] [local-
  filesystem]
  no
  reset-pcap {controlpath-pcap | datapath-pcap}
```

Description

This command enables or disables packet capturing and set packet capturing options for a single packet capture session.

Parameter	Description
controlpath	Enables controlpath packet capture. Captured packets are stored in /var/log/oslog/filter.pcap. NOTE: Only capture to local-filesystem is supported for controlpath capture. Disabled
interprocess	Enables or disables interprocess packet capturing. Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all ports. All CLI ports, which are TCP, are always skipped. Disabled
other	Enable or disable all other types of packets. Disabled
sysmsg	Enable or disable internal messaging packets. Specify up to ten comma-separated opcodes to capture; use <code>all</code> to sniff all opcodes. All CLI ports, which are TCP, are always skipped. Disabled
tcp	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all TCP ports. All CLI ports, which are TCP, are always skipped. Disabled

Parameter	Description
udp	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all UDP ports. All CLI ports, which are TCP, are always skipped. Disabled
copy-to-flash	Copies captured packets to the flash.
controlpath-pcap	Copies controlpath captures. They are saved as controlpath-pcap.tar.gz .
datapath-pcap	Copies datapath captures. They are saved as datapath-pcap.tar.gz .
datapath	Enables datapath packet capture. Captured packets are stored in <code>/var/log/oslog/datapath.pcap</code> or mirrored out of the managed device. Disabled
ipsec <peer-ip>	Enable or disable IPsec packet capturing. Enter the IPsec peer IP address to specify a given peer. NOTE: Capture to local-filesystem is not supported with this option. Disabled
ipsec <peer-ipv6>	Enable or disable IPsec packet capturing. Enter the IPsec peer IPv6 address to specify a given peer. NOTE: Capture to local-filesystem is not supported with this option. Disabled
wifi-client <mac-address> {decrypted encrypted all}	Enable or disable packet capturing from a wifi client. Specify the client device by entering the device's MAC address. Additionally, you can specify what type of traffic captured: decrypted, encrypted, or all. Disabled
destination	Configures the capture destination.
interface <slot/module/port>	Interface in <slot>/<module>/<port> format.
ip-address <ip-address>	Sends packet captures to a specific IP address.
local-filesystem	Stores captured packets on the managed device in pcap files.

Parameter	Description
no	Negates any configured parameter.
reset-pcap	Deletes old pcap files and restarts the active capture.
controlpath-pcap	Deletes old controlpath pcap files and restarts the active controlpath capture.
datapath-pcap	Deletes old datapath pcap files and restarts the active datapath capture.

This command can perform two types of packet capture: controlpath and datapath. Controlpath only captures packet destined for the managed device. Datapath captures packets that are being forwarded by the managed device, such as packets from a wifi client.

Packets can be retrieved through the `tar logs` command; look for the `filter.pcap` or `datapath.pcap` file. This command activates packet capture options on the current session. They are not saved and applied across all reboots.

Related Command

Command	Description
show papi-security	<p>Defines a set of default packet capture options on the control path and saves them in the configuration file. These settings are automatically enabled when the managed device boots up.</p> <p>NOTE: Any settings defined using the packet-capture command overrides packet-capture-defaults.</p>

Example

The following example enables packet capturing for debugging a wireless WEP station doing VPN. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
(host) [/md] (config) #packet-capture sysmsg 30,29,90
(host) [/md] (config) #packet-capture udp 500,4500,1701,1812,1645
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

packet-capture-defaults

```
packet-capture
  controlpath [interprocess {all | <ports>}] [other] [sysmsg {all | <opcodes>}
  [tcp {all | <ports>}] [udp {all | <ports>}]
  datapath {ipsec <peer-ip>} [wifi-client <mac-address> {decrypted | encrypted |
  all}]
  destination [interface <slot/module/port>] [ip-address <ip-address>] [local-
  filesystem]
  no
```

Description

Use this command to enable or disable packet capturing and define a set of default packet capturing options on the control path for debugging purposes.

This command applies to control path packets; not datapath packets. Packets can be retrieved through the `tar log` command; look for the `filter.pcap` file. This command activates packet capture options on the current switch. They are not saved and applied across switches.

Parameter	Description
controlpath	Enables controlpath packet capture. Captured packets are stored in <code>/var/log/oslog/filter.pcap</code> . Only capture to local-filesystem is supported for controlpath capture. Disabled
interprocess	Enables or disables interprocess packet capturing. . Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all ports. All CLI ports, which are TCP, are always skipped. Disabled
other	Enable or disable all other types of packets. Disabled
sysmsg	Enable or disable internal messaging packets. Specify up to ten comma-separated opcodes to capture; use <code>all</code> to sniff all opcodes. All CLI ports, which are TCP, are always skipped. Disabled
tcp	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all TCP ports. All CLI ports, which are TCP, are always skipped. Disabled

Parameter	Description
udp	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use <code>all</code> to sniff all UDP ports. All CLI ports, which are TCP, are always skipped. Disabled
datapath	Enables datapath packet capture. Captured packets are stored in <code>/var/log/oslog/datapath.pcap</code> or mirrored out of the controller. Disabled
ipsec <peer-ip>	Enable or disable IPsec packet capturing. Enter the IPsec peer IP address to specify a given peer. NOTE: Capture to local-filesystem is not supported with this option. Disabled
wifi-client <mac-address> {decrypted encrypted all}	Enable or disable packet capturing from a wifi client. Specify the client device by entering the device's MAC address. Additionally, you can specify what type of traffic captured: decrypted, encrypted, or all. Disabled
destination	Configures the capture destination.
interface <slot/module/port>	Interface in <slot>/<module>/<port> format.
ip-address <ip-address>	Sends packet captures to a specific IP address.
local-filesystem	Stores captured packets on the controller in pcap files.
no	Negates any configured parameter.

Example

The following example sets the default packet capture values to debug a wireless WEP station doing VPN. Once these default settings are defined, you can use the [packet-capture](#) command to enable packet capturing with these values. This example uses the following parameters and values:

- Station up/down: `sysmsg opcode 30`
- WEP key plumbing: `sysmsg opcode 29`
- DHCP: `sysmsg opcode 90`

- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
(host) [mynode] (config)#packet-capture-defaults sysmsg 30,29,90 udp
500,4500,1701,1812,1645
```

Use the show packet-capture command to show the current action and the default values.

```
(host) [mynode] (config)#show packet-capture

Current Active Packet Capture Actions(current switch)
=====
Packet filtering TCP with 2 port(s) enabled:
  2
  1
Packet filtering UDP with 1 port(s) enabled:
  1
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.

Packet Capture Defaults(across switches and reboots if saved)
=====
Packet filtering TCP with 2 port(s) enabled:
  2
  1
Packet filtering UDP with 1 port(s) enabled:
  1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

page

page <length>

Description

This command sets the number of lines of text the terminal will display when paging is enabled. Use this command in conjunction with the `paging` command to specify the number of lines of text to display. For more information on the pause mechanism that stops the command output from printing continuously to the terminal, see [paging on page 1069](#).

If you need to adjust the screen size, use your terminal application to do so.

Parameter	Description
length	Specifies the number of lines of text displayed. 24 - 100

Example

The following example sets 80 as the number of lines of text displayed:

```
(host) [mynode] (config) #page 80
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

paging

paging

Description

This command stops the command output from printing continuously to the terminal. By default, this command is enabled.

With paging enabled, there is a pause mechanism that stops the command output from printing continuously to the terminal.

If paging is disabled, the output prints continuously to the terminal. To disable paging, use the `no paging` command. You must be in enable mode to disable paging.

The paging setting is active on a per-user session. For example, if you disable paging from the CLI, it only affects that session. For new or existing sessions, paging is enabled by default.

You can also configure the number of lines of text displayed when paging is enabled. For more information, see [page on page 1068](#).

If you need to adjust the screen size, use your terminal application to do so.

Example

The following example enables paging:

```
(host) [mynode] (config) #paging
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

pan active-profile

```
pan active-profile  
  profile <profile name>
```

Description

This command makes a Palo Alto Network (PAN) profile active from a set of profiles. Only one PAN profile can be active at a time.

Parameter	Description
profile <profile name>	The name of the PAN profile to be activated.

Example

The following example creates an active PAN profile from a set of profiles.

```
(host) [mynode] (config) #pan active-profile  
(host) [mynode] (Palo Alto Networks Active Profile) #profile default
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

pan profile

```
pan profile <profile-name>
  clone
  firewall host <host> port <port> username <username> passwd <password>
  no
```

Description

This command configures a Palo Alto Networks profile to allow a managed device to communicate with a PAN firewall. This command is used to configure the PAN firewall that the managed device will be communicating with. The username and password must match the name of the admin account configured on the PAN firewall.

Parameter	Description
clone	Name of an existing PAN profile configuration from which parameter values are copied.
firewall	Configures the information for the associated PAN firewall.
host <host>	IP address or hostname of the PAN firewall.
port <port>	Port number of the PAN firewall.
username <username>	The username of the PAN firewall.
passwd <password>	The password of the PAN firewall.
no	Negates any configured parameter.

Example

The following example configures a Palo Alto Networks profile to allow a managed device to communicate with a PAN firewall.

```
(host) [mynode] (config) #pan profile default
(host) [mynode] (Palo Alto Networks Servers Profile "default") #firewall
host 192.0.2.1 port 5642 username axde passwd ZAQ!2wsx
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor

panic

```
panic {clear | info {file <filename> <symbolfile>|nvram <symbolfile>} | list {file <filename>|nvram} | save <filename>}
```

Description

This command manages information created during a system crash. To troubleshoot system crashes, use the `panic save` command to save information from NVRAM into the specified file, then use the `panic clear` command to clear the information from NVRAM.

Parameter	Description
<code>clear</code>	Removes panic information from non-volatile random access memory (NVRAM).
<code>info</code>	Displays the content of specified panic files.
<code>list</code>	Lists panic information in the specified file in flash or in NVRAM.
<code>save</code>	Saves panic information from NVRAM into the specified file in flash.

Example

The following example lists panic information in NVRAM:

```
(host) [mynode] #panic list nvram
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

papi-security

```
papi-security {enhanced-security|key <key>}  
no
```

Description

This command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key, if required.

Parameter	Description
Enhanced-security	Enables PAPI Enhanced Security Disable
Key <key>	Secret key that is used to authenticate messages between systems 10-64 characters
no	Disables the earlier configuration

This command allows you to use advanced options that regulate PAPI communication between Mobility Conductor and managed devices. When enhanced security is enabled, PAPI messages are authenticated at the receiving device and are denied if validation failed.



Mismatch in secret key will affect centralized licensing and AirWave.

One of the ways PAPI messages are authenticated is through a shared secret key. The papi-security command lets you configure a key on the Mobility Conductor and the managed devices. If no key is configured, then the controller uses the default key.



The Mobility Conductor and the managed device must be configured with the same PAPI key.

Example

The following example enables the PAPI Enhanced Security mode:

```
(host)[mynode] (config) #papi-security  
(host)[mynode] (PAPI Security Profile) #enhanced-security
```

The following example configures a new PAPI Enhanced Security key for controllers and AirWave:

```
(host)[mynode] (PAPI Security Profile) #key 1234567890
```

Related Commands

Command	Description
show papi-security	Shows the status of the PAPI Enhanced Security configuration of the controller.
show ipc statistics app-id show ipc statistics app-name	Show the PAPI statistics for messages transmitted, received, signed, validated, denied, and more based on application ID or the application name.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and managed devices.

password-recovery-disable

```
password-recovery-disable  
no ...
```

Description

This command disables the default password recovery feature in the controller. This command can be executed in SSH sessions and serial console sessions with the controller.

Parameter	Description
password-recovery-disable	Disables the default password recovery feature.
no	Enables the default password recovery feature.

Example

The following example shows how to disable the default password recovery user:

```
(host) configure terminal  
Enter Configuration commands, one per line. End with CNTL/Z  
(host) (config) #password-recovery-disable
```

The following example shows how to enable the default password recovery user:

```
(host) configure terminal  
Enter Configuration commands, one per line. End with CNTL/Z  
(host) (config) #no password-recovery-disable
```

Related Commands

Command	Description
show mgmt-user	This command lists the management users configured on the controller and also shows the status of the default password recovery user.
password-recovery-user	This command creates an alternate password recovery user to recover the lost password.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on controller.

password-recovery-user

```
password-recovery-user <username>  
no ...
```

Description

This command creates an alternate password recovery user and disables the default password recovery feature. This command can be executed in SSH sessions and serial console sessions with the controller.

Parameter	Description
<username>	User name for the password recovery user.
no	Deletes the configured password recovery user and enables the default password recovery feature.

Example

The following example shows how to configure the alternate password recovery user:

```
(host) #configure terminal  
Enter Configuration commands, one per line. End with CNTL/Z  
(host) (config) #password-recovery-user recadmin  
Password:*****  
Re-Type password:*****  
(host) (config) #exit
```

The following example shows how to delete the alternate password recovery user:

```
(host) configure terminal  
Enter Configuration commands, one per line. End with CNTL/Z  
(host) (config) #no password-recovery-user
```

Related Commands

Command	Description
show mgmt-user	This command lists the management users configured on the controller and also shows the status of the default password recovery user.
password-recovery-disable	This command disables the default password recovery feature.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on controller.

perf-test server

```
perf-test server
  start
    ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] [tcp [window <window>]] | udp}
    controller {[tcp [window <window>]] | udp}
  stop
    ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] [tcp [window <window>]] | udp}
    controller {[tcp [window <window>]] | udp}
```

Description

This command launches Iperf throughput test.

Parameter	Description
start	Starts Iperf throughput tests in server mode
stop	Stops Iperf throughput tests in server mode
ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] [tcp [window <window>]] udp}	Starts Iperf throughput test on an AP using: [ap-name <ap-name>] : AP name [ip-addr <ip-addr>] : IP address of AP [ip6-addr <ip6-addr>] : IPv6 address of IP [tcp [window <window>]] : Use TCP window size with suffix k for kilo or m for mega udp : Use UDP
controller {[tcp [window <window>]] udp}	Starts Iperf throughput test on a controller using: [tcp [window <window>]] : Use TCP window size with suffix K for kilo or M for mega udp : Use UDP

Example

The following example starts Iperf throughput test on AP **test** using TCP window size 2k:

```
(host) [mynode] #perf-test server start ap ap-name test tcp window 2k
```

Related Command

Command	Description
show perf-test reports	Use this command to view the results of an Iperf throughput test.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

perf-test client

```
perf-test client
  start
    ap {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]} [host
    {<ip>|<ip6>}] [duration <duration>] [parallel <parallel>] [tcp [window
    <window>]] [udp [bandwidth <bandwidth>]]
    controller [host {<ip>|<ip6>}] [duration <duration>] [parallel <parallel>]
    [tcp [window <window>]] [udp [bandwidth <bandwidth>]]
  stop
    ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]}
    controller
```

Description

This command launches lperf throughput test in client mode. This command launches or stops lperf throughput test in client mode.

Parameter	Description
start	Starts lperf throughput tests in client mode.
ap	Starts lperf throughput tests on specified AP in client mode.
ap-name <ap-name>	Specifies name of an AP.
ip-addr <ip-addr>	Specifies IP address of an AP.
ip6-addr <ip6-addr>	Specifies IPv6 address of an AP.
host {<ip> <ip6>}]	Specifies IP or IPv6 address of perf server.
duration <duration>	Specifies time, in seconds, to transmit. Default is 10 and range is 10 to 120.
parallel <parallel>	Specifies number of parallel clients threads to run. This should be less than the number of parallel threads on the server.
tcp [window <window>]	Specifies TCP window size to use.
udp [bandwidth <bandwidth>]]	Specifies UDP bandwidth to use.
controller	Starts lperf throughput tests on specified controller in client mode.
stop	Stops lperf throughput tests in client mode

Example

The following example starts lperf throughput test on an AP named **ap215** using TCP window size 2k in client mode:

```
(host) [mynode] #perf-test client start ap ap-name ap215 host 192.0.2.1
duration 10 parallel 1 tcp window 2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

perf-test port

perf-test port {close|open}

Description

This command closes or opens lperf throughput test port 5001.

Parameter	Description
close	Closes lperf throughput test port 5001.
open	Opens lperf throughput test port 5001.

Example

The following example closes lperf throughput test port 5001:

```
(host) [mynode] #perf-test port close
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

phonehome

```
phonehome
  auto-report
  disable
  enable
  https <from_addr>
  now
  smtp <a.b.c.d> <from_addr> [port <port_num>] {size <max_size>} [user <username>
  pass <password>]
```

Description

This command configures the PhoneHome auto reporting feature. By default, the managed device sends PhoneHome reports to the Activate server using HTTPS. Most deployments should retain the default behavior send PhoneHome reports via Activate. However, if the managed device is behind proxy server and does not have direct access to Internet, PhoneHome should be configured to send reports using SMTP. The following section of this document describes the benefits of each of these configurations options.

Parameter	Description
auto-report	The managed device will periodically contact Aruba support once a week to report any errors or changes to the managed device configuration or inventory. If the managed device has not reported any errors and its configuration file has not changed, no report will be sent. NOTE: Before you enable auto-reporting, you must first enable the PhoneHome feature using the command <code>phonehome enable</code> .
disable	This parameter disables the PhoneHome feature. Phonehome automatic reporting is disabled by default.
enable	This parameter enables the PhoneHome feature.
now	Issue the <code>phonehome now</code> command in enable mode to immediately create and send a report from the managed device to Aruba support. NOTE: Before you use the <code>phonehome now</code> command to create and send a report, you must first access the CLI in config mode and issue the command <code>phonehome enable</code> to enable this feature.

Parameter	Description
https <from_addr>	Configure managed device to send PhoneHome reports to an Activate server using HTTPS. The <from-addr> email address is used to properly identify the user sending the report.
smtp	Configure the SMTP server that will send email messages from the managed device to Aruba support.
<a.b.c.d>	IP address of the SMTP server
<from_addr>	Local email address from which the auto reporting messages will be sent. For example, <i>admin@mycorp.com</i> .
port <port_num>	(Optional) Port number from which the SMTP server will send auto reporting emails. Default port number: 25.
size <max_size>	(Optional) If your SMTP server has a restriction on the size of the emails it can send, use this parameter to specify the maximum size limit. Any reports larger than this limit will be divided into multiple smaller emails.
user <username> pass <password>	(Optional) If your SMTP server requires user authentication before it can send an email message, enter the username and password for a valid user on your network.

Sending Phonehome Reports using Activate

PhoneHome integration with Activate offers following benefits:

- **Simpler configuration.** Phonehome only requires you to configure the email ID of the network administrator managing the device. as Activate already has information to accurately identify your managed device. If a DNS server is not configured on the managed device, PhoneHome will query the public DNS service (8.8.8.8) to resolve the Activate server IP address.
- **Smaller bandwidth requirements.** When the PhoneHome feature sends the report to the Activate server, the PhoneHome report is zipped into a smaller package, then divided into smaller 1MB pieces before being sent to the server using secure HTTPS. Only reports sent to Activate are zipped before they are sent, so reports sent to Activate use less bandwidth than a report sent to a SMTP server.
- **Enhanced error management.** If any individual portion of the report is not successfully received by the Activate server, PhoneHome makes up to three attempts to resend just that portion of the file, rather than resending the entire report. Reports sent via SMTP must be resent in their entirety if any portion is not received by the SMTP server.
- **Automatic removal of old reports.** Once the entire report has been sent to the Activate server, Activate sends an acknowledgment to the managed device, prompting the managed device to delete its local copy of the report.

Sending Reports using SMTP

If you configure the PhoneHome feature to use SMTP, the PhoneHome status reports is sent in an email. When the managed device generates the report email with the PhoneHome data file attachment, it forwards the email to the local SMTP server configured on your local network, which then relays the message to Aruba technical support. If your email server requires the sender to be authenticated before message delivery, the managed device can connect to the SMTP server by supplying the sender's user name and password.

When PhoneHome reports are sent using SMTP, the PhoneHome report attachment is encrypted before it is transmitted to the SMTP server, and is decrypted by Aruba support the report it is received. If the PhoneHome status report email is larger than the maximum email size supported by your SMTP server, the managed device divides the PhoneHome attachment into multiple smaller attachments and sends the report to Aruba in multiple emails. If any individual portion of the report is not successfully received by the SMTP server, PhoneHome resends the entire report.

Example

The following example turns on the PhoneHome feature, enables weekly auto-reports, and identifies the SMTP server to be used by this feature:

```
(host) [mynode] (config) #phonehome enable auto-report smtp 172.21.18.170
admin@mycorp.com
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	The <code>phonehome now</code> command must be issued in enable mode. All other PhoneHome commands require config mode.

ping

ping

ipv6

```
<global-address> [count <count-value>] [df-flag-ipv6] [validate-reply]
[packet-size <size-value>] [interval <interval-value>] [pattern <pattern-
value>] [timeout <timeout-value>] [tos <tos-value>] [ttl <ttl-value>]
[validate-reply] [source [[<source-address>] [mgmt-interface]]]
interface [vlan <vlanid>] <linklocal-address>
<target> [count <count-value>] [df-flag] [validate-reply] [send-amon] [packet-
size <size-value>] [interval <interval-value>] [pattern <pattern-value>] [timeout
<timeout-value>] [tos <tos-value>] [ttl <ttl-value>] [validate-reply] [source
[[<source-address>] [mgmt-interface]]]
```

Description

This command sends ICMP echo packets to the specified IPv4 or IPv6 address.

Parameter	Description
ipv6	Ping specified IPv6 address.
<global-address>	Ping specified global IPv6 address
count <count-value>	Specifies the number of ping packets to send. 1-1000 5
df-flag-ipv6	Sets the do not fragment flag.
dscp <dscp-value>	Set 6 bits of DSCP field in IP header.
interval <interval-value>	Sets the time interval, in seconds, between ping datagrams. 1-60 seconds 1 second

Parameter	Description
<pre>packet-size <size-value></pre>	<p>Specifies the size in bytes of the ping datagram.</p> <p>10-2000 bytes 100 bytes</p>
<pre>pattern <pattern-value></pre>	<p>Specifies the hexadecimal digit pattern.</p> <p>Up to 16 digits</p>
<pre>source [[<source-address>][mgmt-interface]</pre>	<p>Specifies the source interface (management interface, or VLAN ID) for the ping datagram.</p> <p>1-4094</p>
<pre>sweep-range <min size> <max size> <sweep-interval></pre>	<p>The range of echo packets sizes to be varied while sending out echos.</p> <ul style="list-style-type: none"> ▪ min size : Start packet size in range 10 to 1999. ▪ max size : End packet size in range 11 to 2000. ▪ sweep-interval : Interval or spaces between the echoed packets in range 1 to 1990.
<pre>timeout <timeout-value></pre>	<p>Specifies the time, in seconds, to wait for response.</p>

Parameter	Description
	1-10 seconds 2 seconds
tos <tos-value>	Sets 8 bits of traffic class field in IPv6 header. 0-255 0
ttl <tll-value>	Sets the TTL value, in seconds, for the ping datagram. 1-255 seconds 225 seconds
validate-reply	Validates the reply data.
interface	Specifies interface for link-local address.
vlan <vlanid>	Specifies VLAN ID for local-link address.
<linklocal-address>	Specifies IPv6 link-local address.
<target>	Pings specified IP address

Examples

The following example pings 192.0.2.1.

```
(host) [mynode] #ping 192.0.2.1

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max =
0.03/0.0312/0.036 ms
```

The following example pings the specified IPv6 global address:

```
(host) [mynode] #ping ipv6 2001:db8:0:abcd::1

Press 'q' to abort.
Sending 5, 92-byte ICMPv6 Echos to 2001:db8:0:abcd::1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max =
0.03/0.0312/0.036 ms
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>send-amon</code> parameter was added.
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>interval</code>■ <code>t1</code>■ <code>validate-reply</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

pkt-trace acl

```
pkt-trace acl
<name> [enable | disable] [log] [trace-hex-mask <tmask> [log-1]] [trace [recv]
[send] [fast] [bridge] [route] [session] [rtsp] [station] [init] [vlan] [user]
[mcast] [tunnel] [bwm] [nat] [trunk] [cp-dp-sp] [acl-processing] [heap] [event]
[cp-dp-sp-message] [port] [ftp] [icmp-error] [wep-encrypt] [wep-decrypt] [ipsec-
encrypt] [ipsec-decrypt] [ipsec-ctrl] [pptp] [ip-re-assembly] [wep-icmpfr] [dhcp]
[mobility] [peer] [pptp-ctrl] [tkip-encrypt] [tkip-decrypt] [tkip-ctrl] [tkip-
alloc-err] [sip-alg] [skinny] [vocera] [gsi] [aesccm-encrypt] [aesccm-decrypt]
[netad] [xSec-ctrl] [xSec-encrypt] [xSec-decrypt] [tcp-termination] [log-2]
[dpi]]
```

Description

This command is used to trace packets in the datapath. Use this command only under the supervision of Aruba technical support.

Parameter	Description
<name>	Traces packets for the specified access-control list.
enable	Enables packet tracing for the ACL.
disable	Disables packet tracing for the ACL.
log	Writes packet trace data to log file.
tracemask <tmask>	Specify the trace mask. This value will be provided by Aruba technical support.
trace-hex-mask	Configures datapath trace mask in hexadecimal form
<tmask>	Specifies trace mask in hexadecimal form
[log-1]	Writes packet trace data to log file.
trace	Configures datapath trace options.
acl-processing	Trace mask for acl functionality
aesccm-decrypt	Trace mask for aesccm-decrypt functionality
aesccm-encrypt	Trace mask for aesccm-encrypt functionality
bridge	Trace mask for bridge functionality
bwm	Trace mask for bwm functionality

Parameter	Description
cp-dp-sp	Trace mask for control path, slow path and fast path messaging functionality
cp-dp-sp-message	Additional trace mask for control path, slow path and fast path messaging functionality
dhcp	Trace mask for dhcp functionality
dpi	Trace mask for datapath DPI
event	Trace mask for event functionality
fast	Trace mask for fast functionality
ftp	Trace mask for FTP functionality
gsi	Trace mask for GSI functionality
heap	Trace mask for heap functionality
icmp-error	Trace mask for ICMP error processing functionality
init	Trace mask for init functionality
ip-re-assembly	Trace mask for IP re-assembly functionality
ipsec-ctrl	Trace mask for IPsec-ctrl functionality
ipsec-decrypt	Trace mask for IPsec-decrypt functionality functionality
ipsec-encrypt	Trace mask for IPsec-encrypt functionality functionality
log-2	Enables writing packet trace data into log file
mcast	Trace mask for mcast functionality
mobility	Trace mask for mobility functionality
nat	Trace mask for NAT functionality
netad	Trace mask for netad functionality
peer	Trace mask for peer functionality
port	Trace mask for port functionality
pptp	Trace mask for PPTP functionality
pptp-ctrl	Trace mask for PPTP-ctrl functionality
recv	Trace mask for recv functionality

Parameter	Description
route	Trace mask for route functionality
rtsp	Trace mask for rtsp functionality
send	Trace mask for send functionality
session	Trace mask for session functionality
sip-alg	Trace mask for sip alg service functionality
skinny	Trace mask for skinny functionality
station	Trace mask for station functionality
tcp-termination	Trace mask for datapath TCP termination functionality
tkip-alloc-err	Trace mask for TKIP-alloc-err functionality
tkip-ctrl	Trace mask for TKIP-ctrl functionality
tkip-decrypt	Trace mask for TKIP-decrypt functionality
tkip-encrypt	Trace mask for TKIP-encrypt functionality
trunk	Trace mask for trunk functionality
tunnel	Trace mask for tunnel functionality
user	Trace mask for user functionality
vlan	Trace mask for VLAN functionality
vocera	Trace mask for Vocera functionality
wep-decrypt	Trace mask for WEP-decrypt functionality functionality
wep-encrypt	Trace mask for WEP-encrypt functionality functionality
wep-icmpfr	Trace mask for WEP-icmpfr functionality
xSec-ctrl	Trace mask for xSec-ctrl functionality
xSec-decrypt	Trace mask for xSec-decrypt functionality
xSec-encrypt	Trace mask for xSec-encrypt functionality

Example

The following example enables packet tracing for the traffic matching the acl **stateful-dot1x**.

```
(host) [mynode] #pkt-trace acl stateful-dot1x enable trace
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

pkt-trace-global

```
pkt-trace-global
  sbeth
    destination-ip
    destination-mac
    ether-type
    packet-count
    packet-stats
    protocol
    source-ip
    source-mac
    trace-type
  trace
  trace-hex-mask <tmask>
  tuple
    destination-ip
    destination-mac
    ether-type
    packet-count
    protocol
    source-ip
    source-mac
```

Description

This command enables global packet tracing in the datapath. Use this command only under the supervision of Aruba technical support.

Parameter	Description
sbeth	Configure datapath buffer tracing.
destination-ip	Specify the destination IP address (A.B.C.D).
destination-mac	Specify the destination MAC address (AA:BB:CC:DD:EE:FF).
ether-type	Specify the packet ethernet frame type.
packet-count	Specify the number of packets to trace.
packet-stats	Per flow Frame statistics.
protocol	Specify protocol number.
source-ip	Specify source IP address (A.B.C.D).

Parameter	Description
source-mac	Specify source MAC address (AA:BB:CC:DD:EE:FF).
trace-type <1-3>	Specify type of the trace to enable: <ul style="list-style-type: none"> ■ 1: packet based ■ 2: module based ■ 3: both
trace	Specify one of the following datapath trace option: <ul style="list-style-type: none"> ■ acl-processing: Trace Mask for acl functionality ■ aesccm-decrypt: Trace Mask for aesccm-decrypt functionality ■ aesccm-encrypt: Trace Mask for aesccm-encrypt functionality ■ bridge: Trace Mask for bridge functionality ■ bwm: Trace Mask for bwm functionality ■ cp-dp-sp: Trace Mask for control path, slow path and fasth path messaging functionality ■ cp-dp-sp-message: Additional Trace Mask for control path, slow path and fasth path messaging functionality ■ dhcp: Trace Mask for dhcp functionality ■ dpi: Trace Mask for datapath DPI ■ event: Trace Mask for event functionality ■ fast: Trace Mask for fast functionality ■ ftp: Trace Mask for ftp functionality ■ gsi: Trace Mask for gsi functionality ■ heap: Trace Mask for heap functionality ■ icmp-error: Trace Mask for icmp error processing functionality ■ init: Trace Mask for init functionality ■ ip-re-assembly: Trace Mask for IP re-assembly functionality ■ ipsec-ctrl: Trace Mask for ipsec-ctrl functionality ■ ipsec-decrypt: Trace Mask for ipsec-decrypt functionality ■ ipsec-encrypt: Trace Mask for ipsec-encrypt functionality ■ mcast: Trace Mask for mcast functionality ■ mobility: Trace Mask for mobility functionality ■ nat: Trace Mask for nat functionality ■ netad: Trace Mask for netad functionality ■ peer: Trace Mask for peer functionality ■ port: Trace Mask for port functionality ■ pptp: Trace Mask for pptp functionality ■ pptp-ctrl: Trace Mask for pptp-ctrl functionality ■ recv: Trace Mask for recv functionality ■ route: Trace Mask for route functionality ■ rtsp: Trace Mask for rtsp functionality ■ send: Trace Mask for send functionality ■ session: Trace Mask for session functionality

Parameter	Description
	<ul style="list-style-type: none"> ■ sip-alg: Trace Mask for sip alg service functionality ■ skinny: Trace Mask for skinny functionality ■ station: Trace Mask for station functionality ■ tcp-termination: Trace Mask for datapath tcp termination functionality ■ tkip-alloc-err: Trace Mask for tkip-alloc-err functionality ■ tkip-ctrl: Trace Mask for tkip-ctrl functionality ■ tkip-decrypt: Trace Mask for tkip-decrypt functionality ■ tkip-encrypt: Trace Mask for tkip-encrypt functionality ■ trace-hex-mask: Configure Datapath Trace mask in Hex Form ■ trunk: Trace Mask for trunk functionality ■ tunnel: Trace Mask for tunnel functionality ■ user: Trace Mask for user functionality ■ vlan: Trace Mask for vlan functionality ■ vocera: Trace Mask for vocera functionality ■ wep-decrypt: Trace Mask for wep-decrypt functionality functionality ■ wep-encrypt: Trace Mask for wep-encrypt functionality functionality ■ wep-icmpfr: Trace Mask for wep-icmpfr functionality ■ xSec-ctrl: Trace Mask for xSec-ctrl functionality ■ xSec-decrypt: Trace Mask for xSec-decrypt functionality ■ xSec-encrypt: Trace Mask for xSec-encrypt functionality
trace-hex-mask <tmask>	Configure datapath trace mask in Hex format.
tuple	Configure datapath tracing by tuples in packet pipeline.
destination-ip	Specify the destination IP address (A.B.C.D).
destination-mac	Specify the destination MAC address (AA:BB:CC:DD:EE:FF).
ether-type	Specify the packet ethernet frame type.
packet-count	Specify the number of packets to trace.
protocol	Specify protocol number.
source-ip	Specify source IP address (A.B.C.D).
source-mac	Specify source MAC address (AA:BB:CC:DD:EE:FF).

Example

The following example enables the global packet tracing for all traffic.

```
(host) [mynode] (config) #pkt-trace-global
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configure mode on Mobility Conductor.

pkt-trace-rap

```
pkt-trace-rap
  enable
    [[acl <acl>]][global][ingress <ingress>]] [trace-mask <trace-mask>] [[ap-name
  <ap-name>]][ip-addr <ip-addr>]]
```

Description

This command enables packet tracing in RAP datapath.

Parameter	Description
enable	Enables packet tracing in RAP datapath.
acl <acl>	Specifies name of the ACL.
[global]	Traces all packets.
ingress <ingress>	Traces packets from ingress.
trace-mask <trace-mask>	Specifies the trace mask. This value will be provided by Aruba technical support.
ap-name <ap-name>	Specifies name of an AP.
ip-addr <ip-addr>	Specifies IP address of an AP.

Example

The following example enables packet tracing in RAP datapath:

```
(host) [mynode] #pkt-trace-rap enable acl default trace-mask OA ap-name
ap215
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

poe-bounce

```
poe-bounce <slot/module/port>
  time-interval <down-time>
```

Description

This command disables poe for selected interface for specific duration. The default value for which poe is disabled is 3 seconds.

Parameter	Description
<slot/module/port>	Specify the gigabyte interface in <slot>/<module>/<port> format.
time-interval <down-time>	Set the time duration in seconds for poe to be disabled. 3-15

Example

The following example disables the poe for port 1 of gigabyte interface module 1 in slot 1.

```
(host)[mynode] #poe-bounce 1/1/1 time-interval 5
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

policy-domain

```
policy-domain group-profile <name of the profile>
  clone <source>
  controller <ip address> <macaddress>
  controller-v6 <ip address> <macaddress>
  no
```

Description

This command configures a policy domain profile to apply role-based ACL for users present in different controllers.

Only one domain group profile is supported in this release. The command should be executed in the /md node and the policy domain group profile supports IPv4 and IPv6 addresses but a combination of both is not supported.

Parameter	Description
<name of the profile>	Name of the profile.
controller <ip address>	IPv4 address of the controller.
controller-v6 <ip6 address>	IPv6 address of the controller.
<mac address>	Mac address of the controller.
no	Deletes the profile.

Example

The following example configures a policy domain profile,

```
(host) [md] policy-domain group-profile test
(host) [md] (Policy Domain Profile "test") controller 1.1.1.1
00:0a:95:9d:68:16
```

Command History

Release	Modification
ArubaOS 8.7.0.0	A new parameter, <code>clone</code> was added.
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Managed devices.

port-bounce

```
port-bounce <slot/module/port>  
  time-interval <down-time>
```

Description

This command shuts down the selected port for specific duration. The default value for which the port is shut down is 3 seconds.

Parameter	Description
<slot/module/port>	Specify the gigabyte interface in <slot>/<module>/<port> format.
time-interval <down-time>	Set the time duration in seconds for which the port is to be shut down. 3-15

Example

The following example shuts down the port 1 of gigabyte interface module 1 in slot 1 for 6 seconds.

```
(host)[mynode] #port-bounce 1/1/1 time-interval 6
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

pptp ip local pool

```
pptp ip local pool <pool_name> <pool_start_address> [<pool_end_address>]
```

Description

This command configures an IP address pool for VPN users using PPTP. PPTP is an alternative to IPsec that is supported by various hardware platforms. PPTP is considered to be less secure than IPsec but also requires less configuration.

If VPN is used as an access method, you must specify the pool from which the user's IP address is assigned when the user negotiates a PPTP session.

Parameter	Description
<pool-name>	User-defined name for the address pool.
<pool_start_address>	Starting IP address for the pool.
<pool_end_address>	Ending IP address for the pool.

Related Commands

Command	Description
show vpdn pptp local pool	Displays the IP address pool for VPN users using Point-to-Point Tunneling Protocol. Use this command to see the used and free addresses in the pool.
vpdn group pptp	This command configures a PPTP VPN connection.

Example

The following example configures an IP address pool for PPTP VPN users:

```
(host) [mynode] (config) #pptp ip local pool pptp-pool1 172.16.18.1  
172.16.18.24
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

present-working-node

present-working-node

Description

This command shows the full path of the current configuration node.

Example

The following example shows the full path of the current configuration node:

```
(host) [mynode] #present-working-node  
/mm/mynode
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

priority-map

```
priority-map <name>  
  dot1p <priority> high  
  dscp <priority> high  
  no ...
```

Description

This command configures the ToS and CoS values used to map traffic into high priority queues. This command allows you to prioritize inbound traffic that is already tagged with 802.1p or IP ToS in hardware queues. You apply configured priority maps to ports on the managed device (using the `interface gigabitethernet` command). This causes the managed device to inspect inbound traffic on the port; when a matching QoS tag is found, the packet or flow is mapped to the specified queue.

Parameter	Description
<name>	User-defined name of the priority map.
dot1p	IEEE 802.1p priority value, or a range of values separated by a dash (-). 0-7
dscp	DSCP priority value, or a range of values separated by a dash (-). 0-63
no	Negates any configured parameter.

Example

The following example configures a priority map and applies it to a port:

```
(host) [mynode] (config) #priority-map pri1  
dscp 4-20 high  
dscp 60 high  
dot1p 4-7 high  
interface gigabitethernet 0/0/4  
priority-map pri1
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

process monitor

process monitor log|restart|

Description

This command validates the integrity of processes every 120 seconds. If a process does not respond during three consecutive 120-second timeout intervals, that process is flagged as non-responsive and the process monitor will create a log message, restart the process or reboot the managed device.

Parameter	Description
log	The process monitor creates a log message when a process fails to responding properly. This is the default behavior for the process monitor
restart	This parameter enables strict behavior for runtime processes. When you enable this option, the process monitor will restart processes that fail to responding properly.

The CLI command `process monitor log` enables logging for process monitoring. By default, whenever a process does not update a required file or send a heartbeat pulse within the required time limit, the process monitor records a critical log message, but does not restart any process. If you want the configure watchdog to restart a process once it fails to respond, use the `command process monitor restart` command.

Example

The following example changes the default process monitor behavior, so the process monitor restarts nonresponsive processes.

```
(host) [mynode] #process monitor restart
```

The `show process monitor statistics` command displays the current status of all the processes running under the process monitor watchdog. A partial example of the output of this command is shown below:

```
(host) (config) #show process monitor statistics

Process Monitor Statistics
-----
Name                               State           Restarts  Timeout Value
Timeout
```

```

-----
-----
-----
-----
-----
/mswitch/bin/arci-cli-helper  PROCESS_RUNNING 0      120      3
/mswitch/bin/fpcli           PROCESS_RUNNING 0      120      3
/mswitch/bin/packet_filter   PROCESS_RUNNING 0      120      3
/mswitch/bin/certmgr         PROCESS_RUNNING 0      120      3
/mswitch/bin/dbstart         PROCESS_RUNNING 0      120      3
/mswitch/bin/cryptoPOST      PROCESS_RUNNING 0      120      3
/mswitch/bin/sbConsoled      PROCESS_RUNNING 0      120      3
/mswitch/bin/pubsub          PROCESS_RUNNING 0      120      3
/mswitch/bin/cfgm            PROCESS_RUNNING 0      120      3
/mswitch/bin/syslogdwrap     PROCESS_RUNNING 0      120      3
/mswitch/bin/aaa             PROCESS_RUNNING 0      120      3
/mswitch/bin/fpapps          PROCESS_RUNNING 0      120      3
/mswitch/bin/pim             PROCESS_RUNNING 0      120      3
/mswitch/bin/lic

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

process reset

```
process reset wms
```

Description

This command performs an internal soft-reset of the module.

Parameter	Description
wms	WLAN Management System.

Example

```
(host) [mynode] #process reset wms
WARNING: Do you really want to perform an internal soft-reset of this module
[y/n]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

process restart

```
process restart <name> [core]
```

Description

This command restarts a process and optionally creates a core file.

Parameter	Description
<name>	Name of the process to restart.
[core]	Creates a core file

Example

The following example restarts the **dbsync** process and creates a core file:

```
(host) [mynode] #process restart dbsync core
WARNING: Do you really want to restart process: dbsync (y/n): y
Restarting: dbsync
```

The following example restarts the **tm** process and creates a core file:

```
(host) [mynode] #process restart tm
WARNING: Do you really want to restart process: tm (y/n): y
Restarting: tm
```

Command History

Release	Modification
ArubaOS 8.10.0.0	The tm process was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

process snapshot

```
process snapshot <name> <pid>
```

Description

This command interrupts a process temporarily to create a snapshot file.

Parameter	Description
<name>	Name of the process to snapshot.
<pid>	Process id of the process to snapshot.

Example

The following example restarts the **dbsync** process and creates a core file:

```
(host) [mynode] #process snapshot
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

product serial-number

```
product serial-number <sl-num>
```

Description

This command configures the product serial-number for a managed device on a Virtual Machine (VM).

Parameter	Description
<sl-num>	Configure the serial number provided by Aruba.

Before you install ArubaOS on a VM instead of a physical Arubacontroller, contact your Aruba sales representative or authorized reseller and request a VM serial number, then use this serial number as a part of your VM configuration. This serial number is a randomly generated string in the format *DC<7-digit-string>*, for example, **DC0000001**. You must configure the VM serial number and identify the passphrase for that device before you can generate a license key for that specific VM configuration.

Example

The following example configures a product serial-number:

```
(host) [mynode] #product serial-number 0123456789
```

Related Commands

Command	Description
show inventory	Display the Mobility Conductor serial number used to generate licenses for a Mobility Conductor deployment.
show license passphrase	Display the Mobility Conductor passphrase used to generate licenses for a Mobility Conductor deployment.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor or a managed device.

prompt

```
prompt <new-prompt>
```

Description

This command changes the prompt text. You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

You cannot alter the parentheses that surround the prompt text, or the greater-than (>) or hash (#) symbols that indicate user or enable CLI mode.

Parameter	Description
<code>new-prompt</code>	The prompt text displayed by the Mobility Conductor. 1-64 <hostname>

Example

The following example changes the prompt text to "It's a new day!".

```
(host) [mynode] (config) #prompt "It's a new day!"  
(It's a new day!) (config) #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

provision-ap

```
provision-ap
  a-ant-bearing <bearing>
  a-ant-gain <gain>
  a-ant-pol <a-ant-pol>
  a-ant-tilt-angle <angle>
  a-antenna {1|2|both}
  altitude <altitude>
  ap-group <group>
  ap-lldp-pse-detect {disabled|enabled}
  ap-name <name>
  ap-poe-power-optimization
  ap2xx-prestandard-poe-detection
  apdot1x-factory-cert
  apdot1x-passwd <string>
  apdot1x-timeout-bypass
  apdot1x-timeout-retries
  apdot1x-tls
  apdot1x-tls-suffix
  apdot1x-tls-suffix-domain <apdot1x-tls-suffix-domain>
  apdot1x-username <name>
  aruba-modem-apn <aruba-modem-apn>
  aruba-modem-plmn <aruba-modem-plmn>
  cellular_nw_preference 3g-only|4g-only|advanced|auto
  cert-DN
  dns-server-ip <ipaddr>
  dns-server-ip6 <ipv6 address>
  domain-name <name>
  external-antenna
  fqln <name>
  g-ant-bearing <bearing>
  g-ant-gain <gain>
  g-ant-pol <g-ant-pol>
  g-ant-tilt-angle <angle>
  g-antenna {1|2|both}
  gateway <ipaddr>
  gateway6 <ipv6-address>
  ikepsk <key>
  ikepsk-hex-based
  iot-ant-gain <gain>D
  installation default|indoor|outdoor
  ip6addr <ipv6-address>
  ip6prefix <ipv6-prefix>
  ipaddr <ipaddr>
  latitude <location>
  link-priority-cellular <link-priority-cellular>
  link-priority-ethernet <link-priority-ethernet>
  link-priority-wifi <link-priority-wifi>
  longitude <location>
  master/conductor {<name>|<ipaddr>}
  master/conductor-preference <ipv4 | ipv6>
  mesh-role {mesh-auto|mesh-point|mesh-portal|none|remote-mesh-portal}
  mesh-sae {sae-disable|sae-enable}
```

```

netmask <netmask>
no ...
ocsp_default
pap-passwd <string>
pap-user <name>
pkcs12-passphrase <string>
pppoe-chap-secret<key>
pppoe-passwd <string>
pppoe-service-name <name>
pppoe-user <name>
preferred_uplink
radio-0-5ghz-ant-gain <radio-0-5ghz-ant-gain>
radio-0-5ghz-ant-pol <radio-0-5ghz-ant-pol>
radio-1-5ghz-ant-gain <radio-1-5ghz-ant-gain>
radio-1-5ghz-ant-pol <radio-1-5ghz-ant-pol>
remote-ap
read-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
reprovision {all|ap-name <name>|ip-addr <ipaddr>|ip6-addr <ip6-addr>|serial-num
<string>|wired-mac <macaddr>}
reset-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
sch-mode-radio-0
sch-mode-radio-1
sch-mode-radio-6ghz
server-ip <server-ip>
server-name <name>
set-ikepsk-by-addr <ip-addr>
set-trust-anchor
syslocation <string>
trustanchor
uplink-vlan <uplink-vlan>
usb-csr
usb-dev <usb-dev>
usb-dial <usb-dial>
usb-init <usb-init>
usb-passwd <usb-passwd>
usb-power-mode {auto|enable|disable}
usb-tty <usb-tty>
usb-tty-control <usb-tty-control>
usb-type <usb-type>
usb-user <usb-user>
wifi-uplink

```

Description

This command provisions or reprovisions an AP.

You do not need to provision APs before installing and using them. The exceptions are outdoor APs, which have antenna gains that you must provision before they can be used, and APs configured for mesh. You must provision the AP before you install it as a mesh node in a mesh deployment.



Users less familiar with this process may prefer to use the **Provisioning** page in the WebUI to provision an AP.

Provisioned or re-provisioned values do not take effect until the AP is rebooted. APs reboot automatically after they are successfully reprovisioned.

To enable cellular uplink for a Remote AP, the Remote AP must have the device driver for the USB data card and the correct configuration parameters. ArubaOS includes device drivers for the most common hardware types, but you can use the **usb** commands in this profile to configure a Remote AP to recognize and use an unknown USB modem type.

Parameter	Description
a-ant-bearing	<p>Determines the horizontal coverage distance of the 802.11a (5 GHz) antenna from True North.</p> <p>From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern.</p> <p>NOTE: This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.</p> <p>0-360 Decimal Degrees</p>
a-ant-gain	<p>Antenna gain for 802.11a (5GHz) antenna.</p>
a-ant-pol	<p>Antenna polarization value for 5GHz radio. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ 0: CO-Polarized ■ 1: Cross-Polarized
a-ant-tilt-angle	<p>Directs the angle of the 802.11a (5GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt.</p> <p>NOTE: This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.</p> <p>-90 to +90 Decimal Degrees</p>
a-antenna	<p>Antenna use for 5 GHz (802.11a) frequency band. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas (default) <p>1, 2, both</p>

Parameter	Description
	both
altitude	Altitude, in meters, of the AP. NOTE: This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.
ap-group	Name of the AP group to which the AP belongs.
ap-lldp-pse-detect	Enabling causes the AP to detect the POE type via LLDP POE TLV. Use one of the following parameters: <ul style="list-style-type: none"> ■ enabled: The AP uses PSE TYPE in the POE TLV to detect the PSE type. ■ disabled: The AP detects the POE using the HW classification.
ap-name	Name of the AP to be provisioned.
ap-poe-power-optimization	Enables optimization to minimize the POE draw of the AP. Enabling optimization may disable some parts of the AP. Disabling optimization ensures all features are enabled.
ap2xx-prestandard-poe-detection	Configures the pre-standard PoE detection on 200 Series APs. The POE+ pre-standard detection is only available on 200 Series APs. It consists of a basic voltage comparator. If the line voltage is equal to or greater than 51 V, the PSE is assumed to be 802.3at compatible.
apdot1x-factory-cert	Enables AP to use factory certificates when doing 802.1x EAP-TLS.
apdot1x-passwd	Password of the AP to authenticate to 802.1X using PEAP.
apdot1x-timeout-bypass	Enables AP to be provisioned when 802.1X authentication times out.
apdot1x-timeout-retries	Sets the apdot1x timeout threshold. If the auth timeouts over this threshold, the AP will bypass apdot1x auth.
apdot1x-tls	Enables AP to 802.1x using EAP-TLS.

Parameter	Description
apdot1x-tls-suffix	Enables AP to use EAP-TLS username suffix.
apdot1x-tls-suffix-domain <apdot1x-tls-suffix-domain>	Set the suffix domain for AP dot1x EAP-TLS username. If defined, use EAP-TLS username as suffix, else use aruba.ap . 1- 63 string length
apdot1x-username	Username of the AP to authenticate to 802.1X using PEAP.
aruba-modem-apn <aruba-modem-apn>	Configures the APN of Aruba 4G LTE modem.
aruba-modem-plmn <aruba-modem-plmn>	Configures the PLMN of Aruba 4G LTE modem.
cellular_nw_preference 3g-only 4g-only advanced auto	<p>This setting allows you to select how the modem should operate.</p> <ul style="list-style-type: none"> ■ auto (default): In this mode, the modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the Remote AP. ■ 3g_only: Locks the modem to operate only in 3G. ■ 4g_only: Locks the modem to operate only in 4G. ■ advanced: The Remote AP controls the cellular network service selection based on the Received Signal Strength Indication (RSSI) threshold-based approach. Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.

Parameter	Description
cert-DN	The Server Certificate CN for Identity
dns-server-ip	IP address of the DNS server for the AP.
dns-server-ip6	IPv6 address of the DNS server for the AP.
domain-name	Domain name for the AP.
external-antenna	Use an external antenna with the AP.
fqln	FQLN for the AP, in the format <APname.floor.building.campus>.
g-ant-bearing	<p>Determines the horizontal coverage distance of the 802.11g (2.4GHz) antenna from True North.</p> <p>From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern.</p> <p>NOTE: This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.</p> <p>0-360 decimal degrees</p>
g-ant-gain	Antenna gain for 802.11g (2.4GHz) antenna.
g-ant-pol	<p>Antenna polarization value for 2.4GHz radio. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ 0: CO-Polarized ■ 1: Cross-Polarized
g-ant-tilt-angle	<p>Directs the angle of the 802.11g (2.4GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt.</p> <p>NOTE: This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.</p> <p>-90 to +90 Decimal Degrees</p>

Parameter	Description
g-antenna	Antenna use for 2.4 GHz (802.11g) frequency band. Use one of the following parameters: <ul style="list-style-type: none"> ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas 1, 2, both both
gateway	IP address of the default gateway for the AP.
gateway6	IPv6 address of the default gateway for the AP.
ikepsk	IKE preshared key for the AP.
ikepsk-hex-based	Specify if the ikepsk is hex-based or text-based. (set -> Hex, unset -> Text).
iot-ant-gain <gain>	Configures an antenna gain value for APs with external antennas.
installation	Specifies the type of installation (indoor or outdoor). The default parameter automatically selects an installation mode based upon the AP model type. indoor, outdoor
ip6addr	Static IPv6 address of the AP.
ip6prefix	The prefix of static IPv6 address of the AP.
ipaddr	Static IP address for the AP.
latitude	Latitude coordinates of the AP. Use the format: Degrees, Minutes, Seconds (DMS). For example: 37 22 00 N
link-priority-cellular <link-priority-cellular>	Sets the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary link.

Parameter	Description
link-priority-ethernet <link-priority-ethernet>	Sets the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.
link-priority-wifi <link-priority-wifi>	Sets the priority of the Wi-Fi uplink. Both Wi-Fi and wired uplink types have equal priority, depending on their availability. If one of the uplink types is not available, the other uplink type is set as the primary link by default. However if both the uplink types are available, one of them is chosen randomly as the primary link.
longitude	Longitude coordinates of the AP. Use the DMS format. For example: 122 02 00 W
master/conductor	Name or IP address of the Mobility Conductor.
master/conductor-preference	Configures the preferred IP protocol (IPv4 or IPv6) for AP master/ conductor discovery.
mesh-role	Configures the AP to operate as a mesh node. You assign one of four roles: mesh auto , mesh portal , mesh point or remote mesh point . If you select none , the AP operates as a thin AP.
mesh-sae	<p>Enables or disables Simultaneous Authentication of Equals (SAE) on a mesh network. This option offers enhanced security over the default wpa2-psk-aes mesh security setting, and provides secure, attack-resistant authentication using a PSK. SAE supports simultaneous initiation of a key exchange, allowing either party to initiate an exchange or both parties to initiate a key exchange simultaneously</p> <p>To use the SAE feature, you must enable this parameter on all mesh nodes (points and portals) in the network, to prevent mesh link connectivity issues.</p> <p>NOTE: This is a Beta feature only. This parameter should be kept "disabled" for this release.</p>
netmask	Netmask for the IP address.

Parameter	Description
ocsp_default	If this parameter is set to 0 (default accept) and the certificate status is unknown, the server certificate is considered valid and the Remote AP comes up. If this parameter is set to 1 (default deny) and the certificate status is unknown, the server certificate is considered revoked and the Remote AP does not come up. By default, OCSF default is set to 0 (default accept).
no	Negates any configured parameter.
pap-passwd	PAP password for the AP. You can use special characters in the PAP password. Following are the restrictions: <ul style="list-style-type: none"> ■ You cannot use double-byte characters ■ You cannot use a tilde (~) ■ You cannot use a tick (') ■ If you use quotes (single or double), you must use the backslash (\) before and after the password
pap-user	PAP username for the AP.
pkcs12-passphrase	Passphrase in PKCS12 format.
pppoe-chap-secret	PPPoE CHAP secret key for the AP.
pppoe-passwd	PPPoE password for the AP.
pppoe-service-name	PPPoE service name for the AP.
pppoe-user	PPPoE username for the AP.
preferred_uplink	Choose AP preferred uplink interface (eth0-eth1). This is only applicable to AP-318, AP-374, AP-375, and AP-377 access points.
radio-0-5ghz-ant-gain <radio-0-5ghz-ant-gain>	Antenna gain for Radio 0 (5 GHz) antenna. NOTE: This parameter is only needed for APs that support dual 5 GHz mode.
radio-0-5ghz-ant-pol <radio-0-5ghz-ant-pol>	Antenna polarization value for Radio 0 (5 GHz) antenna. Use one of the following parameters:

Parameter	Description
	<ul style="list-style-type: none"> ■ 0: CO-Polarized ■ 1: Cross-Polarized <p>NOTE: This parameter is only needed for APs that support dual 5 GHz mode.</p>
radio-1-5ghz-ant-gain <radio-1-5ghz-ant-gain>	<p>Antenna gain for Radio 1 (5 GHz) antenna.</p> <p>NOTE: This parameter is only needed for APs that support dual 5 GHz mode.</p>
radio-1-5ghz-ant-pol <radio-1-5ghz-ant-pol>	<p>Antenna polarization value for Radio 1 (5 GHz) antenna. Use one of the following parameters:</p> <ul style="list-style-type: none"> ■ 0: CO-Polarized ■ 1: Cross-Polarized <p>NOTE: This parameter is only needed for APs that support dual 5 GHz mode.</p>
read-bootinfo	<p>Retrieves current provisioning parameters of the specified AP.</p> <p>NOTE: This parameter can only be used on the Mobility Conductor.</p>
remote-ap	<p>This is a remote AP.</p>
reprovision	<p>Provisions one or more APs with the values in the provisioning-params workspace. To use reprovision, you must use read-bootinfo to retrieve the current values of the APs into the provisioning-ap-list.</p> <p>NOTE: This parameter can only be used on the Mobility Conductor.</p>
reset-bootinfo	<p>Restores factory default provisioning parameters to the specified AP.</p> <p>NOTE: This parameter can only be used on the Mobility Conductor.</p>

Parameter	Description
sch-mode-radio-0	If you are provisioning an 802.11n-capable AP, you can issue the sch-mode-radio-0 command to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This setting is disabled by default.
sch-mode-radio-1	If you are provisioning an 802.11n-capable AP, you can issue the sch-mode-radio-1 command to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This setting is disabled by default.
sch-mode-radio-6ghz	If you are provisioning an 802.11n-capable AP, you can issue the sch-mode-radio-6Ghz command to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This setting is disabled by default.
server-ip	IPv4 or IPv6 address of the managed device from which the AP boots.
server-name	DNS name of the managed device from which the AP boots.
set-ikepsk-by-addr	Sets a IKE preshared key to correspond to a specific IP address.
set-trust-anchor	Set trust anchor for the AP.
syslocation	User-defined description of the location of the AP.
trustanchor	Name of the trust anchor.
uplink-vlan <uplink-vlan>	<p>If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature.</p> <p>NOTE: If an AP is provisioned with an uplink VLAN, it <i>must be connected to a trunk mode port</i> or the AP's frames will be</p>

Parameter	Description
	dropped.
usb-csr	The USB storage for CSR and private key file.
usb-dev	The USB device identifier, if the device is not already supported.
usb-dial	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
<pre>usb-modeswitch "-v <default_vendor> -p <default_product> -V <target_vendor> -P <target_product> -M <message_content>"</pre>	<p>USB cellular devices on Remote APs typically register as modems, but may occasionally register as a mass-storage device. If a Remote AP cannot recognize its USB cellular modem, use the <code>usb-modeswitch</code> command to specify the parameters for the hardware model of the USB cellular data-card.</p> <p>NOTE: You must enclose the entire modeswitch parameter string in quotation marks.</p>
usb-init	<p>The initialization string for the USB modem. This string configures the AP Name setting of the USB modem. For the USB modem to understand this string, the value entered should adhere to one of the following formats:</p> <ul style="list-style-type: none"> ■ Use double-quotes and prefix them with a backslash character. See example below: "AT+CGDCONT=1,\"IP\", \"APN\"" ■ Use single-quote instead of double-quotes. AP translates single-quote into double-quotes. See example below: "AT+CGDCONT=1,'IP','APN'" ■ Use the string begin-end pair without double quotes. See example below: AT+CGDCONT=1,'IP','APN' <p>■ In some cases, the 4G/LTE modem requires the configuration of two AP Names during USB initialization. The first AP Name initiates the connection to obtain an IP address, and the second AP Name sends and receives</p>

Parameter	Description
	<p>data. Use the ; delimiter character to create two separate strings for the AP Names in the command. See example below:</p> <pre>"AT+CGDCONT=1,\"IP\", \"APN1\";1,1,\"APN2\""</pre> <p>NOTE: You must obtain the AP Name from your ISP and ensure that each AP Name entry follows the manufacturer's AT command reference.</p>
usb-passwd	A PPP password, if provided by the cellular service provider
usb-power-mode auto enable disable	Sets the USB power mode to control the power to the USB port.
usb-tty	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
usb-tty-control	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.
usb-type	<p>Specify the USB driver type.</p> <ul style="list-style-type: none"> ■ acm: Use ACM driver ■ airprime: Use Airprime driver ■ beceem-wimax: Use Beceem driver for 4G-WiMAX ■ ether: Use CDC Ether driver for direct IP 4G device ■ hso: Use HSO driver for newer Option ■ none: Disable 3G or 2G network on USB ■ option: Use Option driver ■ pantech-3g: Same as "pantech-uml290" - to support upgrade ■ pantech-uml290: Use Pantech USB driver for UML290 device ■ ptumlbnet: Use Pantech USB driver for 4G device ■ rndis: Use a RNDIS driver for a 4G device ■ sierra-evdo: Use EVDO Sierra Wireless driver ■ sierra-gsm: Use GSM Sierra Wireless driver ■ sierrausbnet: Use SIERRA Direct IP driver for 4G device

Parameter	Description
	<ul style="list-style-type: none"> ■ storage: Use USB flash as storage device for storing Remote AP certificates
usb-user	The PPP username provided by the cellular service provider.
wifi-uplink	Enables the AP to use Wi-Fi uplink.

Provisioning a Single AP

To provision a single AP:

1. Use the **read-bootinfo** option to read the current information from the deployed AP you wish to re-provision.
2. Use the **show provisioning-ap-list** command to see the AP to be provisioned.
3. Use the **copy-provisioning-params** option to copy the AP's parameter values to the provisioning-params workspace.
4. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
5. Use the **reprovision** option to provision the AP with the values in provisioning-params workspace. The AP automatically reboots.

Provisioning Multiple APs at a Time

You can change parameter values for multiple APs at a time, however, note the following:

- You cannot provision the following AP-specific options on multiple APs:
 - ap-name
 - ipaddr
 - pap-user
 - pap-passwd
 - ikepsk
 - If any of these options are already provisioned on the AP, their values are retained when the AP is re-provisioned.
- The values of the server-name, a-ant-gain, or g-ant-gain options are retained if they are not re-provisioned.
- All other values in the provisioning-params workspace are copied to the APs.

To provision multiple APs at the same time:

1. Use the **read-bootinfo** to read the current information from each deployed AP that you wish to provision.



The AP parameter values are written to the provisioning-ap-list. To reconfigure multiple APs, the APs must be present in the provisioning-ap-list. Use the **show provisioning-ap-list** command to see the APs that will be provisioned. Use the **clear provisioning-ap-list** command to clear the provisioning-ap-list.

2. Use the **copy-provisioning-params** option to copy an AP's parameter values to the provisioning-params workspace.
3. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
4. Use the **reprovisionall** option to provision the APs in the provisioning-ap-list with the values in provisioning-params workspace. All APs in the provisioning-ap-list automatically reboot.

The following are useful commands when provisioning one or more APs:

- `show|clear provisioning-ap-list` displays or clears the APs that will be provisioned.
- `show|clear provisioning-params` displays or resets values in the provisioning-params workspace.
- `show ap provisioning` shows the provisioning parameters an AP is currently using.

Example

The following example changes the IP address of the Mobility Conductor on the AP:

```
(host) [mynode] (config) #provision-ap
(host) [mynode] (config-submode)read-bootinfo ap-name lab103
(host) [mynode] (config-submode)show provisioning-ap-list
(host) [mynode] (config-submode)copy-provisioning-params ap-name lab103
(host) [mynode] (config-submode)master/ conductor 10.100.102.210
(host) [mynode] (config-submode)reprovision ap-name lab103
```

The following example configures the preferred IP protocol for AP master/ conductor discovery:

```
(host) [mynode] (config) #provision-ap
(host) [mynode] (config-submode)master/ conductor -preference ipv4
```

The following example configures the APN and PLMN of Aruba MDM-USB-LTE 4G modem:

```
(host) [mynode] (config) #provision-ap
(host) [mynode] (config-submode) #aruba-modem-apn <aruba-modem-apn>
(host) [mynode] (config-submode) #aruba-modem-plmn <aruba-modem-plmn>
```


Command History

Release	Modification
ArubaOS 8.10.0.0	The following parameters were introduced: <ul style="list-style-type: none">■ <code>aruba-modem-apn <aruba-modem-apn></code>■ <code>aruba-modem-plmn <aruba-modem-plmn></code>■ <code>iot-ant-gain <gain></code>
ArubaOS 8.8.0.0	The following parameters were introduced: <ul style="list-style-type: none">■ <code>apdot1x-timeout-bypass</code>■ <code>apdot1x-timeout-retries</code>
ArubaOS 8.7.0.0	The <code>master-preference</code> parameter was introduced.
ArubaOS 8.5.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>link-priority-wifi</code>■ <code>wifi-uplink</code>
ArubaOS 8.4.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>apdot1x-tls-suffix</code>■ <code>apdot1x-tls-suffix-domain</code>■ <code>mesh-auto</code>■ <code>preferred_uplink</code>
ArubaOS 8.3.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>radio-0-5ghz-ant-gain</code>■ <code>radio-0-5ghz-ant-pol</code>■ <code>radio-1-5ghz-ant-gain</code>■ <code>radio-1-5ghz-ant-pol</code>
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none">■ <code>apdot1x-factory-cert</code>■ <code>apdot1x-tls</code>■ <code>a-ant-pol</code>■ <code>g-ant-pol</code>■ <code>ap-lldp-pse-detect</code>
ArubaOS 8.1.0.0	The <code>server-ip</code> parameter was modified to accept IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, except for the parameters noted in the syntax table.	Base operating system, except for the parameters noted in the syntax table.	Config mode on Mobility Conductor.

pwd

pwd

Description

This command displays the full path of the current configuration node.

Example

The following example indicates that the current node-path is **/mm/mynode**:

```
(host) [mynode] (config) #pwd
/mm/mynode
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

read-bootinfo

```
read-bootinfo {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{wired-  
mac <wired-mac>}
```

Description

This command retrieves the current provisioning parameters of an AP.

Parameter	Description
ap-name <ap-name>	Retrieves the current provisioning parameters of an AP for specified AP name.
ip-addr <ip-addr>	Retrieves the current provisioning parameters of an AP for specified IP address.
ip6-addr <ip6-addr>	Retrieves the current provisioning parameters of an AP for specified IPv6 address.
wired-mac <wired-mac>	Retrieves the current provisioning parameters of an AP for specified wired MAC address.

Example

The following example retrieves the current provisioning parameters of an AP named ap-205:

```
(host) [mynode] #read-bootinfo ap-name ap-205
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

reload

```
reload
  force
  device-mac
```

Description

This command reboots the managed device if required after making configuration changes or under the guidance of Aruba Networks customer support. The `reload` command powers down the managed device, making it unavailable for configuration. After the managed device reboots, you can access it over a local console connected to the serial port, or through an SSH, Telnet, or WebUI session.

Starting from ArubaOS 8.11.0.0, the **reload** command can be issued only from the **/mm** and **/mm/mynode** nodes of the Mobility Conductor.

Parameter	Description
<code>force</code>	Forces reboot without waiting for confirmation.
<code>device-mac</code>	Specifies the device MAC address for reboot.

Example

The following restarts the managed device without waiting for confirmation:

```
(host) [mynode] #reload force
System will now restart!
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The command can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

reload-peer-sc

reload-peer-sc

Description

This command reboots the peer Supervisor Card if required after making configuration changes or under the guidance of Aruba Networks customer support.

This command is available for chassis system only.

Example

```
(host) [mynode] #reload-peer-sc
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The command can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

rename

```
rename <filename> <newfilename>
```

Description

This command renames an existing system file on the controller. You can use a combination of numbers, letters, and punctuation (periods, underscores, and dashes) to rename a file. The new name takes affect immediately.

Make sure the renamed file uses the same file extension as the original file. If you change the file extension, the file may be unrecognized by the system. For example, if you have an existing file named `upgrade.log`, the new file must include the `.log` file extension.

You cannot rename the active configuration currently selected to boot the controller. If you attempt to rename the active configuration file, the controller returns the following message:

```
Cannot rename active configuration file
```

To view a list of system files, and for more information about the directory contents, see [dir on page 589](#).

Parameter	Description
<code>filename</code>	An alphanumeric string that specifies the current name of the file on the system.
<code>newfilename</code>	An alphanumeric string that specifies the new name of the file on the system.

Example

The following command changes the file named **test_configuration** to **deployed_configuration**:

```
(host) [mynode] (config) #rename test_configuration deployed_configuration
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

reprovision

```
reprovision {wired-mac <wired-mac> | ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr> | serial-num <serial-num> | all}
```

Description

This command sends current provisioning-profile to access points.

Parameter	Description
all	Reprovisions all access points listed in provisioning_ap_list
ap-name <ap-name>	Reprovisions an AP with the specified AP name.
ip-addr <ip-addr>	Reprovisions an AP with the specified IP address.
ip6-addr <ip6-addr>	Reprovisions an AP with the specified IPv6 address.
serial-num <serial-num>	Reprovisions an AP with the specified serial number.
wired-mac <wired-mac>	Reprovisions an AP with the specified MAC address.

Example

Access the CLI and use the following command to reprovision an AP **test**:

```
(host) [mynode] #reprovision ap-name test
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

reset-bootinfo

```
reset-bootinfo
  ap-name
  ip-addr
  wired-mac
```

Description

This command restores the factory default values for an access point.

Parameter	Description
ap-name <ap-name>	Restores the factory default values for the specified name of the access point.
ip-addr <ip-addr>	Restores the factory default values for the specified IP address of the access point.
wired-mac <wired-mac>	Restores the factory default values for the specified MAC address of the AP.

Example

Access the CLI and use the following command to restore factory default values for an access point with MAC address **00:1a:1e:aa:bb:cc**:



```
(host) [mynode] #reset-bootinfo wired-mac 00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

replace-config-reboot

```
replace-config-reboot <filename1> <config-path1> <filename2> <config-path2>
```

Description

This command is used to replace the configuration in a stand-alone controller and the controller will reboot with provided configuration file. The replace-config-reboot command also copies the current node config of /mm/mynode and /mm nodes to the corresponding backup files named mynode_replace_reboot_backup and mm_replace_reboot_backup respectively.

```
(VMC) [mynode] #dir
-rw-r--r--    1 root  root   42974 Oct 14 04:39 mynode_replace_reboot_backup
-rw-r--r--    1 root  root  114345 Aug  8 23:58 mm_replace_reboot_backup
```

Parameter	Description
filename1	The name of the configuration file in flash directory of stand-alone controller
filename2	The name of the configuration file in flash directory of stand-alone controller
config-path1	If configuration file has to be applied only at /mm node then set <config-path1> to /mm.
config-path2	If configuration file has to be applied only at /mm/mynode node then set <config-path1> to /mm/mynode.

Example

Below command will apply the template files at /mm and /mm/mynode nodes.

Applying template files at /mm node and at /mm/mynode node

```
(standalone) [mynode] (config) #configuration node replace-config-reboot
mmfile.cfg /mm mdfile.cfg /mm/mynode
Controller will be rebooted with provided configuration file. An improper
configuration might prevent controller to come up. Do you wish to continue ?
[y/n]: y
(VMC) [mynode] (config) #
(VMC) [mynode] (config) #
[11:39:59]:Starting reboot me
[11:39:59]:Shutdown processing started
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	config mode on stand-alone controllers.

restore

```
restore
  config
  factory_default
  flash
```

Description

This command restores the file or configuration. Use the `backup flash` command to tar and compress flash directories to the `flashbackup.tar.gz` file.

Parameter	Description
<code>config</code>	Restores configuration directories from a <code>configbackup.tar.gz</code> file.
<code>factory_default</code>	Restores factory default settings.
<code>flash</code>	Restores important directories from <code>flashbackup.tar.gz</code> file.

Example

The following command restores directories from the `flashbackup.tar.gz` file:

```
(host) [mynode] #restore flash
Please wait while we restore the flash backup.....
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

rf am-scan-profile

```
<profile-name>  
  clone <profile>  
  dwell-time-active-channel  
  dwell-time-dos-channel  
  dwell-time-other-reg-domain-channel  
  dwell-time-rare-channel  
  dwell-time-reg-domain-channel  
  no  
  scan-mode
```

Description

Configure an Air Monitor (AM) scanning profile. Channels are categorized into the following types:

Active Channel: This qualifier indicates that wireless activity (for example, a probe request) is detected on this channel by the presence of an AP or other 802.11 activity.

All Regulatory Domain Channels: A valid non-overlapping channel that is in the regulatory domain of at least one country.

Rare Channels: Channels that fall into a frequency range outside of the regulatory domain; 2484 MHz and 4900MHz-4995MHz (J-channels), and 5000-5100Mhz.

Regulatory Domain Channels: A channel that belongs to the regulatory domain of the country in which the AP is deployed. The set of channels that belong to this group is a subset of the channels in all-reg-domain channel group.

Parameter	Description
<profile-name>	Name of this instance of the profile. 1-63 characters
clone <profile>	Copy data from another AM scanning profile
dwell-time-active-channel	Dwell time (in ms) for channels where there is wireless activity. 100-32768 ms 500 ms
dwell-time-dos-channel	Dwell time (in ms) to contain rogue devices. 100-32768 ms 500 ms
dwell-time-other-reg-domain-channel	Dwell time (in ms) for channels not in the APs regulatory domain. 100-32768 ms

Parameter	Description
	250 ms
<code>dwell-time-rare-channel</code>	Dwell time (in ms) for rare channels. 100-32768 ms 100 ms
<code>dwell-time-reg-domain-channel</code>	Dwell time (in ms) for AP's Regulatory domain channels 100-32768 ms 250 ms
<code>no</code>	Delete the command
<code>scan-mode</code>	Set the scanning mode for the radio.
<code>all-reg-domain</code>	Scan channels in all regulatory domain
<code>rare</code>	Scan <i>all</i> channels (all regulatory domains and rare channels)
<code>reg-domain</code>	Scan channels in the APs regulatory domain

Command History

Release	Modification
ArubaOS 8.5.0.0	The <code>dwell-time-dos-channel</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	RFProtect.	Config mode on Mobility Conductor.

rft

```
rft test profile ht-link-quality ap-name <ap-name> [dest-mac <dest-mac> [radio {0|1}mcs]]
```

```
rft test profile link-quality {ap-name <ap-name> dest-mac <dest-mac> [phy {a|g}|radio {0|1}] | bssid <bssid> dest-mac <dest-mac> | ip-addr <ip-addr> dest-mac <macaddr> [phy {a|g}|radio {0|1} | ip6-addr <ip6-addr> dest-mac <macaddr> [phy {a|g}|radio {0|1}]]
```

```
rft test profile raw {ap-name <name> dest-mac <dest-mac> [phy {a|g}|radio {0|1}] | bssid <bssid> dest-mac <dest-mac> | ip-addr <ip-addr> dest-mac <dest-mac> [phy {a|g}|radio {0|1}]]
```

Description

This command is used for RF troubleshooting. This command can run predefined test profiles for antenna connectivity, link quality, or raw testing. You should only run these commands when directed to do so by an Aruba support representative.

Parameter	Description
ap-name	Name of the AP that performs the test.
dest-mac	MAC address of the client to be tested.
phy	802.11 type, either a or g. a g
radio	Radio ID, either 0 or 1.
bssid	BSSID of the AP that performs the test. 0 1
ip-addr	IP address of the AP that performs the test.
ip6-addr	IPv6 address of the AP that performs the test.

Command History

Version	Modification
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none">■ ht-link-quality■ ip6-addr
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf arm-rf-domain-profile

```
rf arm-rf-domain profile
  arm-rf-domain-key <arm-rf-domain-key>
```

Description

This profile holds a non-editable key defined by Mobility Conductor, and used to sign over-the air (OTA) ARM updates exchanged between APs.

Parameter	Description
<arm-rf-domain-key>	Non-editable key value

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf arm-profile

```
rf arm-profile <profile>
  40MHz-allowed-bands {All|None|a-only|g-only}
  80MHz support
  160MHz support {Auto|Contiguous-only|Non-contiguous-only|None}
  acceptable-coverage-index <number>
  active-scan (not intended for use)
  aggressive-scan
  assignment {disable|maintain|multi-band|single-band}
  backoff-time <seconds>
  channel-quality-aware-arm
  channel-quality-threshold <channel-quality-threshold>
  channel-quality-wait-time <seconds>
  client-aware
  client-match
  clone <profile>
  cm-6ghz-band-steer
  cm-band-a-min-signal <cm-band-a-min-signal>
  cm-band-g-max-signal <cm-band-g-max-signal>
  cm-dot11v
  cm-he-min-signal
  cm-he-pooling-signal-delta <cm-he-pooling-signal-delta>
  cm-he-pooling-snr-thresh <cm-he-pooling-snr-thresh>
  cm-lb-client-thresh <#-of-clients>
  cm-lb-interval <cm-lb-interval>
  cm-lb-signal-delta <cm-lb-signal-delta>
  cm-lb-snr-thresh <dB>
  cm-lb-thresh <%-of-clients>
  cm-max-steer-fails <#-of-fails>
  cm-mu-client-thresh <count>
  cm-mu-snr-thresh <value>
  cm-report-interval
  cm-stale-age <secs>
  cm-steer-backoff <secs>
  cm-steer-timeout <secs>
  cm-sticky-check_intvl <secs>
  cm-sticky-min-signal <-dB>
  cm-sticky-snr <dB>
  cm-sticky-snr-delta
  cm-update-interval <dB>
  cm-unst-ageout-interval days <days> hours <hours>
  cm-unst-ageout
  default-6ghz
  dynamic-bw
  dynamic-bw-beacon-failed-thresh <dynamic-bw-beacon-failed-thresh>
  dynamic-bw-cca-ibss-thresh <dynamic-bw-cca-ibss-thresh>
  dynamic-bw-cca-intf-thresh <dynamic-bw-cca-intf-thresh>
  dynamic-bw-clear-time <dynamic-bw-clear-time>
  dynamic-bw-wait-time <dynamic-bw-wait-time>
  error-rate-threshold <percent>
  error-rate-wait-time <seconds>
  free-channel-index <number>
  high-noise-backoff-time <high-noise-backoff-time>
```

```

ideal-coverage-index <number>
interfering-ap-weight <number>
load-aware-scan-threshold
max-tx-power <dBm>
min-scan-time <# of scans>
min-tx-power <dBm>
mode-aware
multi-band-scan
no ...
ota-updates
ps-aware-scan
radar-backoff-time <radar-backoff-time>
rogue-ap-aware
scan mode {all-reg-domain|reg-domain}
scan-interval
scanning
video-aware-scan
voip-aware-scan
voip-aware-scan-timer

```

Description

This command configures the Adaptive Radio Management (ARM) profile. Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that allows each AP to determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. This command configures an ARM profile that you apply to a radio profile for the 5 GHz or 2.4 GHz frequency band (see [rf dot11a-radio-profile on page 1196](#) or [rf dot11g-radio-profile on page 1228](#)).

Parameter	Description
<profile>	Name of this instance of the profile. The name must be 1-63 characters. default
40MHz-allowed-bands	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band. All/None/ a-only/g-only a-only
All	Allows 40 MHz channels on both the 5 GHz (802.11a) and 2.4 GHz (802.11b/g) frequency bands.
None	Disallows use of 40 MHz channels.

Parameter	Description
a-only	Allows use of 40 MHz channels on the 5 GHz (802.11a) frequency band only.
g-only	Allows use of 40 MHz channels on the 2.4 GHz (802.11b/g) frequency band only.
80MHz-support	If enabled, 80 MHz channels can be used in the 5 GHz frequency band on APs that support 802.11ac. enabled
160MHz support	Specifies which 160 MHz mode to be assigned. This parameter does not apply to 2.4 GHz frequency band.
Auto	Allows automatic selection of contiguous frequency.
Contiguous-only	Allows to assign contiguous only 160 MHz channel bandwidth.
Non-contiguous-only	Allows to assign non-contiguous 160 MHz channel bandwidth.
None	This sub-parameter disallows assigning 160 MHz channel bandwidth.
acceptable-coverage-index	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. This setting applies to multi-band implementations only. 1-6 4
active-scan	When active-scan is enabled, an AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. This feature is disabled by default, and should <i>not be enabled</i> except under the direct supervision of Aruba Technical Support. disabled
aggressive-scan	When this feature is enabled, an AP radio with no clients will scan channels every second. enabled
assignment	Activates one of four ARM channel/power assignment modes. single-band (new installations only)

Parameter	Description
disable	Disables ARM channel/power assignments.
maintain	Maintains existing channel assignments.
multi-band	Computes ARM assignments for both 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.
single-band	Computes ARM assignments for a single band.
backoff-time	Time, in seconds, an AP backs off after requesting a new channel or power. 120-3600 240 sec
channel-quality-aware-arm	If enabled, ARM changes are based upon an internally calculated channel quality metric. When this feature is disabled, ARM initiates channel changes based on thresholds defined in this profile, and chooses the channel based on the calculated interference index value. disabled
channel-quality-threshold	Channel quality percentage below which ARM initiates a channel change. 0-100 70
channel-quality-wait-time	If channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change. 1-3600 120
client-aware	If the Client Aware option is enabled, the AP does not change channels if there is active client traffic on that AP. If Client Aware is disabled, the AP may change to a more optimal channel, but this change may also disrupt current client traffic. enabled
client match	ClientMatch helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless client's probe requests.

Parameter	Description
	<p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.</p> <p>enabled</p>
clone	Name of an existing ARM profile from which parameter values are copied.
cm-6ghz-band-steer	Enable or disable Client Match band steers to 6GHz.
cm-band-a-min-signal <cm-band-a-min-signal>	<p>Minimum signal level required for the targeted A band radio in a Client Match band steer move (-dBm).</p> <p>0-255 dbm</p> <p>75</p>
cm-band-g-max-signal <cm-band-g-max-signal>	<p>Maximum signal level of the G band radio that can trigger a Client Match band steer move (-dBm)</p> <p>0-255 dbm</p> <p>45</p>
cm-dot11v	<p>Client Match steers using 802.11v BSS Transition Management.</p> <p>enabled</p>
cm-he-min-signal	<p>Minimum signal required for the targeted HE move (-dbm).</p> <p>0-255 dbm</p> <p>55</p>
cm-he-pooling-signal-delta	Target radio should not have weaker signal strength than current source radio by the configured value.
cm-he-pooling-snr-thresh	Client match HE pooling SNR threshold (dB) at target radio
cm-lb-client-thresh <#-of-clients>	<p>If an AP radio has fewer clients than the client match load balancing threshold defined by this parameter, the AP will not participate in load balancing.</p> <p>0-100 clients</p> <p>30</p>

Parameter	Description
cm-lb-interval <cm-lb-interval>	<p>Controls how often client load balancing will be done (in minutes). Set to 0 to disable Load Balancing.</p> <p>0-255 minutes 5 minutes</p>
cm-lb-signal-delta	<p>Client match will not move a client to a new radio if the signal strength of the target AP is this dB value lower than the radio to which the client is currently associated. This parameter works differently than the cm-lb-snr-thresh value, which imposes a definite value on the target AP's signal-to-noise ratio. the cm-lb-signal-delta imposes a <i>relative</i> constraint based upon the signal strength of the radio to which the client is currently associated.</p> <p>0-20 dB 5 dB</p>
cm-lb-snr-thresh <dB>	<p>Clients must detect a SNR from an underutilized AP radio at or above this threshold before ClientMatch considers load balancing a client to that radio.</p> <p>0-100 dB 25</p>
cm-lb-thresh <%-of-clients>	<p>When ClientMatch is enabled, clients may be steered from a highly utilized channel on an AP to a channel with fewer clients. If a channel on an AP radio has this percentage fewer clients than another channel supported by the client, ClientMatch may move clients from the busier channel to the channel with fewer clients.</p> <p>0-100% 20</p>
cm-max-steer-fails <#-of-fails>	<p>The controller keeps track of the number of times ClientMatch failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If ClientMatch attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger.</p> <p>This parameter defines the maximum allowed number of client match steering fails with the same trigger before the client is marked as unsteerable for that trigger.</p> <p>0-100 failures 5</p>

Parameter	Description
cm-mu-client-thresh <count>	<p>Total number of clients that can be associated to a radio, in which the radio can still be considered for multi-user (MU) steering.</p> <p>0-255 dbm</p> <p>15</p>
cm-mu-snr-thresh <value>	<p>Minimum SNR value of a client on the target radio, in which the radio can still be considered for multi-user (MU) steering.</p> <p>0-255 dbm</p> <p>30</p>
cm-report-interval <secs>	<p>This interval defines how often an AP sends an updated client probe report to the controller. Each client probe report contains a list of MAC addresses for clients that have been active in the last two minutes, and the AP radio SNR values seen by those clients.</p> <p>0-255 secs</p> <p>30</p>
cm-stale-age <secs>	<p>The controller can maintain client match data for the maximum number of supported clients for that controller platform, showing the detected SNR values for up to 16 candidate APs per client. This table is periodically updated as APs send client probe reports to the controller. This parameter defines the amount of time that the controller should retain client match data from each client probe report.</p> <p>Different controller types support varying numbers of clients.</p> <ul style="list-style-type: none"> ■ 7005: 1024 client ■ 7010: 2048 clients ■ 7030: 4096 clients ■ 7240: 32000 clients ■ 7220: 24000 clients ■ 7210: 16000 clients <p>0- 65535 seconds</p> <p>120 seconds</p>
cm-steer-backoff	<p>Client Match will attempt one IOS steer at the configured backoff time interval.</p>
cm-steer-timeout	<p>When a client is steered from one AP to a more desirable AP, the steer timeout feature helps facilitate the move by defining the amount of time that any APs to which the client should NOT associate will not respond to the AP.</p>

Parameter	Description
	0-255 seconds
cm-sticky-check-interval <secs>	Frequency at which the AP checks for client's received SNR values. If the SNR value drops below the threshold defined by the <code>cm-sticky-snr</code> parameter for three consecutive check intervals, that client may be moved to an different AP. 0-255 seconds 3 seconds
cm-sticky-min-signal <-dB>	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the candidate AP radio is at or higher than the minimum signal level defined by this parameter <i>and</i> the candidate radio has a higher signal strength than the radio to which the client is currently associated. (The required improvement in signal strength can be defined using the <code>cm-sticky-snr-delta</code> command.) 0-255 (-dB) 65
cm-sticky-snr <dB>	If the client's received signal strength indicator (RSSI) is above this signal-to-noise ratio (SNR) threshold, that client will be allowed to stay associated to its current AP. If the client's received signal strength is below this threshold, it may be moved to a different AP. 0-255 dB
cm-sticky-snr-delta	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the AP radio is stronger than its current radio by the dB level defined by the <code>cm-sticky-snr-thresh</code> parameter, and the candidate radio also has a minimum signal level defined by the <code>cm-sticky-min-signal</code> parameter. 0-100 dB 10
cm-unst-ageout-interval days <days>	The client entries in an unsteerable client list remain in effect for the interval defined by this parameter before they age out. 2 days

Parameter	Description
cm-unst-ageout	<p>When client match and the client match unsteerable client ageout feature are enabled, the controller periodically sends APs that are not a desired AP match for a client in a list of unsteerable clients. These lists contain a list of MAC addresses for up to 128 clients that should not be steered to that AP. The following controller types support a aggregate maximum of unsteerable clients for all APs associated to that controller.</p> <ul style="list-style-type: none"> ■ 7005: 256 unsteerable clients ■ 7010: 512 unsteerable clients ■ 7030: 1024 unsteerable clients ■ 7240: 8000 unsteerable clients ■ 7220: 6000 unsteerable clients ■ 7210: 4000 unsteerable clients
default-6ghz	<p>Configures the ARM default-6 GHz profile. For more information, see rf arm-profile default-6ghz.</p>
dynamic-bw	<p>Issue the <code>dynamic-bw</code> parameter to enable the ARM dynamic bandwidth switch feature. When enabled ARM can detect 20MHz interferers that can impact an AP radio using an 80MHz channel and move the AP radio to another 80MHz channel. For more information, see 80 MHz Dynamic Bandwidth Switch on page 1165</p> <p>disabled</p>
dynamic-bw-beacon-failed-thresh	<p>The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the number of failed beacons exceeds this value during the observation window.</p> <p>1-500 30</p>
dynamic-bw-cca-ibss-thresh	<p>The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel assignment IBSS percentage drops below this value during the observation window.</p> <p>1-100 10</p>
dynamic-bw-cca-intf-thresh	<p>The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel assignment interference percentage exceeds this value during the observation window.</p> <p>1-100 30</p>

Parameter	Description
dynamic-bw-clear-time	<p>The ARM dynamic bandwidth switch feature returns the AP radio to 80MHz channel after this clear time period if there is no high volume of traffic.</p> <p>1-300 seconds</p> <p>30</p>
dynamic-bw-wait-time	<p>Minimum time in seconds dynamic bandwidth switch indicators have to be true to trigger a 80MHz to 40MHz bandwidth change.</p> <p>1-300 seconds</p> <p>30</p>
error-rate-threshold	<p>The percentage of errors in the channel that triggers a channel change. Recommended value is 50%. A value of 0% disables this feature.</p> <p>0-100</p> <p>default-a: 70%, default-g: 70%</p>
error-rate-wait-time	<p>Time, in seconds, that the error rate has to be at least the error rate threshold to trigger a channel change. Recommended values are 1-100.</p> <p>1-2,147,483,647</p> <p>default-a: 90 seconds, default-g: 90 seconds</p>
free-channel-index	<p>The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.</p> <p>10-40</p> <p>default-a: 40, default-g: 25</p>
high-noise-backoff-time	<p>The duration, in minutes, for blacklisting/denylisting AirMatch Solver's channel after 2 consecutive high noise detections. Setting the value to 0 disables the backoff window.</p> <p>0-3600</p> <p>720 minutes (12 hours)</p>
ideal-coverage-index	<p>The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. Recommended value is 10.</p> <p>2-20</p> <p>default-a: 6, default-g: 6</p>

Parameter	Description
load-aware-scan-threshold	<p>Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high. The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. The supported range for this setting is 0-20000000 bytes/second. (Specify 0 to disable this feature.)</p> <p>1250000 bytes/second</p>
max-tx-power	<p>Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.</p> <p>3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127</p> <p>default-a: 18 dBm, default-g: 9 dBm</p>
min-scan-time	<p>Minimum number of times a channel must be scanned before it is considered for assignment. The supported range for this setting is 0-2,147,483,647 scans. Best practices are to configure Minimum Scan Time between 1-20 scans. Recommended values are 1-20.</p> <p>1-2,147,483,647</p> <p>8 scans</p>
min-tx-power	<p>Minimum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory minimum. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.</p> <p>3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127</p> <p>default-a: 12 dBm, default-g: 6 dBm</p>
mode-aware	<p>If enabled, ARM will turn APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).</p> <p>disabled</p>

Parameter	Description
multi-band-scan	When enabled, single-radio APs try to scan across bands for rogue AP detection. enabled
no	Negates any configured parameter.
ota-updates	The ota-updates option allows an AP to get information about its RF environment from its neighbors, even the AP cannot scan. If this feature is enabled, when an AP on the network scans a foreign (non-home) channel, it sends other APs an Over-the-Air (OTA) update in an 802.11 management frame that contains information about the scanning AP's home channel, the current transmission EIRP value of its home channel, and one-hop neighbors seen by that AP. enabled
ps-aware-scan	When enabled, the AP will not scan if Power Save is active. disabled
radar-backoff-time	The duration, in minutes, for blacklisting/denylisting AirMatch solver's channel after 2 consecutive radar detections. Setting the value to 0 disables the backoff window. 0-3600 720 minutes (12 hours)
rogue-ap-aware	When enabled, the AP will try to contain off-channel rogue APs. disabled
scan-interval	If scanning is enabled, the scan interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired. Recommended values are 0-30 seconds. 0-2,147,483, 647 seconds 10 seconds
scan-mode	Select the scan mode for the AP: <ul style="list-style-type: none"> ■ all-reg-domain: The AP scans channels within

Parameter	Description
	<p>all regulatory domains. This is the default setting.</p> <ul style="list-style-type: none"> ■ reg-domain: Limit the AP scans to just the regulatory domain for that AP. <p>all-reg-domain</p>
scanning	<p>The Scanning check box enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features:</p> <ul style="list-style-type: none"> ■ Multi Band Scan ■ Rogue AP Aware ■ Voip Aware Scan ■ Power Save Scan <p>Do not disable Scanning unless you want to disable ARM and manually configure AP channel and transmission power.</p> <p>enabled</p>
video-aware-scan	<p>As long as there is at least one video frame every 100 mSec the AP will reject an ARM scanning request. Note that for each radio interface, video frames must be defined in one of two ways:</p> <ul style="list-style-type: none"> ■ Classify the frame as video traffic via a session ACL. ■ Enable WMM on the WLAN's SSID profile and define a specific DSCP value as a video stream. Next, create a session ACL to tag the video traffic with the that DSCP value. <p>enabled</p>
voip-aware-scan	<p>Aruba's VoIP Intelligent Call Handling (ICH) prevents any single AP from becoming congested with voice calls. When you enable ICH, you should also enable voip-aware-scan parameter in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that scanning is also enabled.</p> <p>disabled</p>
voip-aware-scan-timer	<p>When enabled, the AP will not scan if the scan request falls within the scan timer of the last voice frame. Range is 50 ms—1000 ms.</p> <p>Default: 50 ms</p>

Default Profiles

ArubaOS includes two default ARM profiles, **default-a** for 5 Ghz radios, and **default-g** for 2.4 GHz radios.

Channel Quality

Hybrid APs and Spectrum Monitors determine channel quality by measuring channel noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of Wi-Fi retries. Regular APs using ARM derive channel quality values by measuring the noise floor for that channel.

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature is recommended over the legacy bandsteering and spectrum load balancing features, which, unlike client match, do not trigger AP changes for clients already associated to an AP.



Legacy 802.11a/b/g devices do not support ClientMatch. When client match is enabled on 802.11n-capable devices, ClientMatch overrides any settings configured for the legacy bandsteering, station handoff assist or load balancing features. 802.11ac-capable devices do not support the legacy bandsteering, station hand off or load balancing settings, so these APs must be managed on using client match.

When this feature is enabled on an AP, that AP is responsible for measuring the RF health of its associated clients. The AP receives and collects information about clients in its neighborhood, and periodically sends this information to the controller. The controller aggregates and maintains a database of information about AP transmit power levels, client transmit power levels and AP RSSI levels as seen by clients. The controller shares this database with the APs (for their associated clients) and the APs use the information to compute the client-based RF neighborhood and determine which APs should be considered candidate APs for each client. When the controller receives a client steer request from an AP, the controller identifies the optimal AP candidate and manages the client's relocation to the desired radio. This is an improvement from previous releases, where ARM was managed exclusively by APs, the without the larger perspective of the client's RF neighborhood.

The following client/AP mismatch conditions are managed by ClientMatch:

Load Balancing: Client match balances clients across APs on different channels, based upon the client load on the APs and the SNR levels the client detects from an underutilized AP. If an AP radio can support additional clients, the AP will participate in client match load balancing and clients can be directed to that AP radio, subject to predefined SNR thresholds.

Sticky Clients: ClientMatch also helps mobile clients that tend to stay associated to an AP despite low signal levels. APs using client match continually monitor the client's RSSI as it roams between APs, and move the client to an AP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.

Band Steering/Band Balancing: APs using ClientMatch monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 GHz radio, the controller will attempt to steer the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the AP retains a suitable distribution of clients on each of its radios.

■E Steering: 802.11ax clients are best compatible with 802.11ax capable radios, resulting in better throughput and spectral efficiency. When an 802.11ax client is associated with a lower radio, ClientMatch pushes the client to the best compatible 802.11ax radio for advanced capabilities. Though STA is in good health, and is 802.11ax capable, it still sometimes connects to lower radios. ClientMatch finds a potential 802.11ax radio on the same band and the client moves to the new 802.11ax radio.

80 MHz Dynamic Bandwidth Switch

If an AP radio uses an 80 MHz channel, the radio only sends out frames out when the entire 80 MHz channel is clear, even if the AP is sending only a 20 MHz management frame or 40MHz data frame. As a result, throughput on the selected 80 MHz channel can be negatively impacted if interference occurs on both 20 MHz channels of the secondary 40MHz channel.

The ARM dynamic bandwidth switch feature allows ARM to detect the 20MHz interferers in this situation, and potentially move the AP radio to another 80MHz channel, or change the AP transmissions to 40MHz, and use the primary 40MHz channel instead.

When this feature is enabled, ARM starts a dynamic bandwidth switch observation window if load-aware scan rejects increase, *and* the clear channel assignment IBSS percentage (the percentage of channel traffic sent from that AP radio) drops below the value defined by the `dynamic-bw-cca-ibss-thresh` parameter.

If an observation window opens, and the clear channel assignment interference threshold exceeds the value defined by the `dynamic-bw-cca-intf-thresh` parameter, and the number of failed beacons from the radio exceeds the threshold defined by the `dynamic-bw-beacon-failed-thresh` parameter during that observation period, ARM will move the AP to another available 80MHz channel with the minimum interference index. If no other 80MHz channel is available, ARM downgrades the radio bandwidth to 40MHz.

ARM Scanning

The default ARM scanning interval is determined by the `scan-interval` parameter in the ARM profile. If the AP does not have any associated clients (or if most of its clients are inactive) ARM will dynamically readjust this default scan interval, allowing the AP obtain better information about its RF neighborhood by scanning non-home channels more frequently. If an AP attempts to scan a non-home channel but is unsuccessful, the AP will make additional attempts to rescan that channel before skipping it and continuing on to other channels.

Using Adaptive Radio Management (ARM) in a Mesh Network

When a mesh portal operates on a mesh network, the mesh portal determines the channel used by the mesh feature. When a mesh point locates an upstream mesh portal, it will scan the regulatory domain channels list to determine the channel assigned to it, for a mesh point always uses the channel selected by its mesh portal. However, if a mesh portal uses an ARM profile enabled with a single-band or multi-band channel/power assignment and the scanning feature, the mesh portal will scan the configured channel lists and the ARM algorithm will assign the proper channel to the mesh portal.

If you are using ARM in your network, it is important to note that mesh points, unlike mesh portals, do not scan channels. This means that once a mesh point has selected a mesh portal or an upstream mesh point, it will tune to this channel, form the link, and will not scan again unless the mesh link gets broken. This provides good mesh link stability, but may adversely affect system throughput in networks with mesh portals and mesh points. When ARM assigns optimal channels to mesh portals, those portals use different channels, and once the mesh network has formed and all the mesh points have selected a portal (or upstream mesh point), those mesh points will not be able to detect other portals on other channels that could offer better throughput. This type of suboptimal mesh network may form if, for example, two or three mesh points select the same mesh portal after booting, form the mesh network, and leave a nearby mesh portal without any mesh points. Again, this will not affect mesh functionality, but may affect total system throughput.

Example

The following command configures VoIP-aware scanning for the arm-profile named "voice-arm:"

```
(host) [mynode] (config) #rf arm-profile voice-arm
                        voip-aware-scan
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>default-6ghz</code> parameter was added.
ArubaOS 8.8.0.0	The <code>voip-aware-scan-timer</code> parameter was added.
ArubaOS 8.7.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>cm-he-pooling-signal-delta</code> ■ <code>cm-he-pooling-snr-thresh</code>
ArubaOS 8.5.0.0	The <code>cm-he-min-signal</code> parameter was added.
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>high-noise-backoff-time</code> ■ <code>radar-backoff-time</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf arm-profile default-6ghz

```

rf arm-profile default-6ghz
  160MHz support {Auto|Contiguous-only|Non-contiguous-only|None}
  40MHz-allowed-bands {2.4GHz-and-5GHz|2.4GHz-and-6GHz|5GHz-and-6GHz|6GHz-only|a-
only|All|g-only|none}
  80MHz support
  acceptable-coverage-index <acceptable-coverage-index>
  active-scan
  aggressive-scan
  assignment {disable|maintain|multi-band|single-band}
  backoff-time <backoff-time>
  channel-quality-aware-arm
  channel-quality-threshold <channel-quality-threshold>
  channel-quality-wait-time <channel-quality-wait-time>
  client-aware
  client-match
  clone
  cm-6ghz-band-steer
  cm-band-a-min-signal <cm-band-a-min-signal>
  cm-band-g-min-signal <cm-band-g-min-signal>
  cm-dot11v
  cm-he-min-signal <cm-he-min-signal>
  cm-he-pooling-signal-delta <cm-he-pooling-signal-delta>
  cm-he-pooling-snr-thresh <cm-he-pooling-snr-thresh>
  cm-lb-client-thresh <cm-lb-client-thresh>
  cm-lb-interval <cm-lb-interval>
  cm-lb-signal-delta <cm-lb-signal-delta>
  cm-lb-snr-thresh <cm-lb-snr-thresh>
  cm-lb-thresh <cm-lb-thresh>
  cm-max-steer-fails <cm-max-steer-fails>
  cm-mu-client-thresh <cm-mu-client-thresh>
  cm-mu-snr-thresh <cm-mu-snr-thresh>
  cm-report-interval <cm-report-interval>
  cm-stale-age <cm-stale-age>
  cm-steer-backoff <cm-steer-backoff>
  cm-steer-timeout <cm-steer-timeout>
  cm-sticky-check-interval <cm-sticky-check-interval>
  cm-sticky-min-signal <cm-sticky-min-signal>
  cm-sticky-snr <cm-sticky-snr>
  cm-sticky-snr-delta <cm-sticky-snr-delta>
  cm-unst-ageout
  cm-unst-ageout-intvl days <days> hours <hours>
  dynamic-bw
  dynamic-bw-beacon-failed-thresh <dynamic-bw-beacon-failed-thresh>
  dynamic-bw-cca-ibss-thresh <dynamic-bw-cca-ibss-thresh>
  dynamic-bw-cca-intf-thresh <dynamic-bw-cca-intf-thresh>
  dynamic-bw-clear-time <dynamic-bw-clear-time>
  dynamic-bw-wait-time <dynamic-bw-wait-time>

```

```

error-rate-threshold <error-rate-threshold>
error-rate-wait-time <error-rate-wait-time>
free-channel-index <free-channel-index>
gateway
geolocation
gsm
guest-access-email
ideal-coverage-index <ideal-coverage-index>
interfering-ap-weight <interfering-ap-weight>
load-aware-scan-threshold <load-aware-scan-threshold>
max-tx-power {12|127|15|18|21|24||27|3|30|33|6|9}
min-scan-time <min-scan-time>
min-tx-power {12|127|15|18|21|24||27|3|30|33|6|9}
mode-aware
multi-band-scan
no
ota-updates
ps-aware-scan
rogue-ap-aware
scan-interval <scan-interval>
scan mode {all-reg-domain|reg-domain}
scanning
telnet {cli|soe}
threshold {controlpath-cpu|controlpath-memory|datapath-cpu|no-of-APs|no-of-
locals|no-of-VAPs|total-tunnel-capacity|user-capacity}
time-range {absolute|periodic}
time-range-profile <profile-name>
traceoptions
tunnel-group <tungrpname>
tunnel-loop-prevention
tunnel-node-mtu <tnode-mtu>
tunneled-node-address <tnode-ip-address>
ucc {custom-sip|facetime|h323|ich|jabber|noe|rtpa-config|sccp|session-idle-
timeout|sip|skype4b|teams|vocera|webrtc|wificalling}
upgrade-profile
uplink {cellular|health-check|load-balance|wired}
user-role <string>
video-aware-scan
voip-aware-scan
voip-aware-scan-timer
web-cc global-bandwidth-contract {web-cc-category <string>|web-cc-reputation
{high-risk {downstream|upstream}|low-risk {downstream|upstream}|moderate-risk
{downstream|upstream}|suspicious {downstream|upstream}|trustworthy
{downstream|upstream}}}}
web-proxy server <name>
web-server profile
webcc {connectiontype|distributed}
websocket clearpass
wlan {}

```

Description

This command configures the Adaptive Radio Management (ARM) default-6 GHz profile. Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that allows each

AP to determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. This command configures an ARM profile that you apply to a default-6 GHz radio profile.

Parameter	Description
160MHz support Auto Contiguous-only Non-contiguous-only None	Specifies which 160 MHz mode is assigned. Does not apply to the 2.4 GHz radio. Default: None
40MHz-allowed-bands 2.4GHz-and-5GHz 2.4GHz-and-6GHz 5GHz-and-6GHz 6GHz-only a-only All g-only none	Specifies on which bands (802.11a or 802.11g) the 40 MHz channels may be used: <ul style="list-style-type: none"> ■ 2.4GHz-and-5GHz: Allows the use of the 40 MHz channels on both 2.4 GHz and 5 GHz frequency band only. ■ 2.4GHz-and-6GHz: Allows the use of the 40 MHz channels on both 2.4 GHz and 6 GHz frequency band only. ■ 5GHz-and-6GHz: Allows the use of the 40 MHz channels on both 5 GHz and 6 GHz frequency band only. ■ 6GHz: Allows the use of the 40 MHz channels on the 6 GHz frequency band only. ■ A-only: Allows the use of the 40 MHz channels on the 5 GHz (802.11a) frequency band only. ■ All: Allows the 40 MHz channels on both the 5 GHz (802.11a) and 2.4 GHz (802.11b/g) frequency bands. ■ G-only: Allows the use of the 40 MHz channels on the 2.4 GHz (802.11b/g) frequency band only. ■ None: Disallows the use of the 40 MHz channels Default: a-only
80MHz support	If enabled, the 80 MHz channels are used on the 5 GHz radio. Does not apply to the 2.4 GHz radio. Default: Enabled
acceptable-coverage-index	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. This setting applies to multi-band implementations only.
active-scan	When active-scan is enabled, an AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. This feature is disabled by default, and should <i>not be enabled</i> except under the direct supervision of Aruba Technical Support.

Parameter	Description
	Default: Disabled
aggressive-scan	If enabled, an AP radio with no clients will scan channels every second. Default: Enabled
assignment disable maintain multi-band single-band	Specify one of four ARM channel/power assignment modes: Disable: Disable ARM channel/power assignments. Maintain: Maintain existing channel assignments. Single-band: Compute ARM assignments for a single band. Multi-band: Compute ARM assignments for both 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands. Default: Single-band
backoff-time	Time, in seconds, when an AP backs off after requesting a new channel or power. Range: 120-3600 Default: 240
channel-quality-aware-arm	If enabled, ARM changes are based upon an internally calculated channel quality metric. When this feature is disabled, ARM initiates channel changes based on thresholds defined in this profile, and chooses the channel based on the calculated interference index value. Default: Disabled
channel-quality-threshold	Channel quality percentage below which ARM initiates a channel change. Range: 0-100 Default: 70
channel-quality-wait-time	If channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change. Range: 1-3600 Default: 120
client-aware	If the Client Aware option is enabled, the AP does not change channels if there is active client traffic on that AP. If Client Aware is disabled, the AP may change to a more optimal channel, but this change may also disrupt current client traffic. Default: Enabled
client-match	ClientMatch helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless client's probe requests.

Parameter	Description
	If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.
clone	Name of an existing ARM profile from which parameter values are copied.
cm-6ghz-band-steer	Enable Client Match band steers to the 6 GHz radio.
cm-band-a-min-signal	Minimum signal level required for the targeted A band radio in a Client Match band steer move (-dBm). Range: 0-255 dbm Default: 75
cm-band-g-max-signal	Maximum signal level of the G band radio that can trigger a Client Match band steer move (-dBm) Range: 0-255 dbm Default: 45
cm-dot11v	Client Match steers using 802.11v BSS Transition Management. Default: Enabled
cm-he-min-signal	Minimum signal required for the targeted HE move (-dbm). Range: 0-255 dbm Default: 55
cm-he-pooling-signal-delta	Target radio should not have weaker signal strength than current source radio by the configured value.
cm-he-pooling-snr-thresh	Client match HE pooling SNR threshold (dB) at target radio
cm-lb-client-thresh	If an AP radio has fewer clients than the client match load balancing threshold defined by this parameter, the AP will not participate in load balancing. Range: 0-100 Default: 30
cm-lb-interval	Specify, in minutes, how often client load balancing is performed. Range: 0-255 Default: 5

Parameter	Description
cm-lb-signal-delta	<p>Client match will not move a client to a new radio if the signal strength of the target AP is this dB value lower than the radio to which the client is currently associated. This parameter works differently than the cm-lb-snr-thresh value, which imposes a definite value on the target AP's signal-to-noise ratio. The cm-lb-signal-delta imposes a <i>relative</i> constraint based upon the signal strength of the radio to which the client is currently associated.</p> <p>Range: 0-20 Default: 5</p>
cm-lb-snr-thresh	<p>Clients must detect a SNR from an underutilized AP radio at or above this threshold before ClientMatch considers load balancing a client to that radio.</p> <p>Range: 0-100 Default: 25</p>
cm-lb-thresh	<p>Client Match load balancing client distribution threshold between channels, as a percentage of clients.</p>
cm-max-steer-fails	<p>The controller keeps track of the number of times ClientMatch failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If ClientMatch attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger. This parameter defines the maximum allowed number of client match steering fails with the same trigger before the client is marked as unsteerable for that trigger.</p> <p>Range: 0-100 Default: 5</p>
cm-mu-client-thresh	<p>Total number of clients that can be associated to a radio, in which the radio can still be considered for multi-user (MU) steering.</p> <p>Range: 0-255 Default: 15</p>
cm-mu-snr-thresh	<p>Minimum SNR value of a client on the target radio, in which the radio can still be considered for multi-user (MU) steering.</p> <p>Range: 0-255 Default: 30</p>
cm-report-interval	<p>This interval defines how often an AP sends an updated client probe report to the controller. Each client probe report contains a list of MAC addresses for clients that have been active in the last two minutes, and the AP radio SNR values seen by those clients.</p> <p>Range: 0-255 Default: 30</p>

Parameter	Description
cm-stale-age	<p>The controller can maintain client match data for the maximum number of supported clients for that controller platform, showing the detected SNR values for up to 16 candidate APs per client. This table is periodically updated as APs send client probe reports to the controller. This parameter defines the amount of time, in seconds, that the controller should retain client match data from each client probe report.</p> <p>Different controller types support varying numbers of clients.</p> <ul style="list-style-type: none"> ■ 7005: 1024 client ■ 7010: 2048 clients ■ 7030: 4096 clients ■ 7240: 32000 clients ■ 7220: 24000 clients ■ 7210: 16000 clients <p>Range: 0-65535 Default: 120 seconds</p>
cm-steer-backoff	<p>Client Match will attempt one IOS steer at the configured backoff time interval.</p>
cm-steer-timeout	<p>When a client is steered from one AP to a more desirable AP, the steer timeout feature helps facilitate the move by defining the amount of time that any APs to which the client should NOT associate will not respond to the AP.</p> <p>Range: 0-255</p>
cm-sticky-check-interval	<p>Frequency at which the AP checks for client's received SNR values. If the SNR value drops below the threshold defined by the <code>cm-sticky-snr</code> parameter for three consecutive check intervals, that client may be moved to an different AP.</p> <p>Range: 0-255 Default: 3</p>
cm-sticky-min-signal	<p>A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the candidate AP radio is at or higher than the minimum signal level defined by this parameter <i>and</i> the candidate radio has a higher signal strength than the radio to which the client is currently associated. (The required improvement in signal strength can be defined using the <code>cm-sticky-snr-delta</code> command.)</p> <p>Range: 0-255 Default: 65</p>
cm-sticky-snr	<p>If the client's received signal strength indicator (RSSI) is above this signal-to-noise ratio (SNR) threshold, that client will be allowed to stay associated to its current AP. If the client's received signal strength is below this threshold, it may be moved to a different AP.</p>

Parameter	Description
	Range: 0-255
cm-sticky-snr-delta	<p>A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the AP radio is stronger than its current radio by the dB level defined by the cm-sticky-snr-thresh parameter, and the candidate radio also has a minimum signal level defined by the cm-sticky-min-signal parameter.</p> <p>Range: 0-100 Default: 10</p>
cm-unst-ageout-intvl days	<p>The client entries in an unsteerable client list remain in effect for the interval, in days and hours, defined by this parameter before they age out.</p> <p>Range: 2</p>
cm-unst-ageout	<p>When client match and the client match unsteerable client ageout feature are enabled, the controller periodically sends APs that are not a desired AP match for a client in a list of unsteerable clients. These lists contain a list of MAC addresses for up to 128 clients that should not be steered to that AP.</p> <p>The following controller types support a aggregate maximum of unsteerable clients for all APs associated to that controller.</p> <ul style="list-style-type: none"> ■ 7005: 256 unsteerable clients ■ 7010: 512 unsteerable clients ■ 7030: 1024 unsteerable clients ■ 7240: 8000 unsteerable clients ■ 7220: 6000 unsteerable clients ■ 7210: 4000 unsteerable clients
dynamic-bw	<p>Issue the dynamic-bw parameter to enable the ARM dynamic bandwidth switch feature. When enabled ARM can detect 20 MHz interferers that can impact an AP radio using an 80 MHz channel and move the AP radio to another 80 MHz channel. For more information, see rf arm-profile default-6ghz on page 1167</p> <p>Default: Disabled</p>
dynamic-bw-beacon-failed-thresh	<p>The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the number of failed beacons exceeds this value during the observation window.</p> <p>Range: 1-500 Default: 30</p>
dynamic-bw-cca-ibss-thresh	<p>The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel assignment IBSS percentage drops below this value during the observation window.</p> <p>Range: 1-100</p>

Parameter	Description
	Default: 10
dynamic-bw-cca-intf-thresh	The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel assignment interference percentage exceeds this value during the observation window. Range: 1-100 Default: 30
dynamic-bw-clear-time	The ARM dynamic bandwidth switch feature returns the AP radio to 80 MHz channel after this clear time period , in seconds, if there is no high volume of traffic. Range: 1-300 Default: 30
dynamic-bw-wait-time	Minimum time in seconds dynamic bandwidth switch indicators have to be true to trigger a 80 MHz to 40MHz bandwidth change. Range: 1-300 Default: 30
error-rate-threshold	The percentage of errors in the channel that triggers a channel change. Recommended value is 50%. A value of 0% disables this feature. Range: 0-100 Default: 70
error-rate-wait-time	Time, in seconds, that the error rate has to be at least the error rate threshold to trigger a channel change. Recommended values are 1-100. Default: 90
free-channel-index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25. Range: 10-40 Default: 40
gateway	Specify the default gateway to use.
geolocation	Specify the geographical location of the device.
gsm	Specify the GSM related tracing.
guest-access-email	Specify the guest-access email profile.
ideal-coverage-index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. Recommended value is 10. Range: 2-20

Parameter	Description
	Default: 6
<code>interfering-ap-weight</code>	The weight of the interfering APs in interference index calculation. Range: 0-100 Default: 25
<code>load-aware-scan-threshold</code>	Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high. The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. The supported range for this setting is 0-20000000 bytes/second. (Specify 0 to disable this feature.) Range: 1250000 bytes/second
<code>max-tx-power</code>	Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. Range: 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127 Default: 18
<code>min-scan-time</code>	Minimum number of times a channel must be scanned before it is considered for assignment. The supported range for this setting is 0-2,147,483,647 scans. Best practices are to configure Minimum Scan Time between 1-20 scans. Range: 1-20. Default: 8
<code>min-tx-power</code>	Minimum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory minimum. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. Range: 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127 Default: 12
<code>mode-aware</code>	If enabled, ARM will turn APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart). Default: Disabled

Parameter	Description
multi-band-scan	When enabled, single-radio APs try to scan across bands for rogue AP detection. Default: Enabled
no	Negates any configured parameter.
ota-updates	The ota-updates option allows an AP to get information about its RF environment from its neighbors, even the AP cannot scan. If this feature is enabled, when an AP on the network scans a foreign (non-home) channel, it sends other APs an Over-the-Air (OTA) update in an 802.11 management frame that contains information about the scanning AP's home channel, the current transmission EIRP value of its home channel, and one-hop neighbors seen by that AP. Default: Enabled
ps-aware-scan	When enabled, the AP will not scan if Power Save is active. Default: Disabled
rogue-ap-aware	When enabled, the AP will try to contain off-channel rogue APs. Default: Disabled
scan-interval	If scanning is enabled, the scan interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired. Range: 0-30 Default: 10
scan-mode	Select the scan mode for the AP: <ul style="list-style-type: none"> ■ all-reg-domain: The AP scans channels within all regulatory domains. This is the default setting. ■ reg-domain: Limit the AP scans to just the regulatory domain for that AP. Default: All-reg-domain
scanning	The Scanning check box enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features: <ul style="list-style-type: none"> ■ Multi Band Scan ■ Rogue AP Aware ■ Voip Aware Scan ■ Power Save Scan

Parameter	Description
	Do not disable Scanning unless you want to disable ARM and manually configure AP channel and transmission power. Default: Enabled
telnet	Enable the telnet port.
threshold	Specify the threshold.
time-range	Specify the time range.
time-range-profile	Specify the time range profile.
traceoptions	Specify the trace options.
tunnel-group	Specify the tunnel group.
tunnel-loop-prevention	Prevent forwarding loops between the tunnels from the tunneled nodes on the managed device.
tunnel-node-mtu	Specify the MTU for the tunneled node.
tunneled-node-address	Specify the IP address of the managed device to terminate the tunnels. An IP address of th 0.0.0.0 disables the configuration.
ucc	Specify the UCC configuration.
upgrade-profile	Specify the upgrade profile.
uplink	Specify the uplink manager configuration.
user-role	Specify the user role.
video-aware-scan	As long as there is at least one video frame every 100 mSec the AP will reject an ARM scanning request. Note that for each radio interface, video frames must be defined in one of two ways: <ul style="list-style-type: none"> ■ Classify the frame as video traffic via a session ACL. ■ Enable WMM on the WLAN's SSID profile and define a specific DSCP value as a video stream. Next, create a session ACL to tag the video traffic with the that DSCP value. Default: Enabled

Parameter	Description
voip-aware-scan	Aruba's VoIP Intelligent Call Handling (ICH) prevents any single AP from becoming congested with voice calls. When you enable ICH, you should also enable voip-aware-scan parameter in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that scanning is also enabled. Default: Disabled
voip-aware-scan-timer	When enabled, the AP will not scan if the scan request falls within the scan timer, in milliseconds, of the last voice frame. Range: 50-1000 Default: 50

Example

The following command configures VoIP-aware scanning for the arm-profile named "voice-arm:"

```
(host) [mynode] (config) #rf arm-profile default-6ghz
```

Command History

Release	Modification
ArubaOS 8.9.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf dot11-6ghz-radio-profile

```
rf dot11-6gHz-radio-profile <profile>
  6ghz-advertise-ap-name
  6ghz-dot11k-enable
  6ghz-mbo-enable
  6ghz-rrm-ie-profile <profile-name>
  advertise-location-6ghz
  am-scan-profile <profile-name>
  arm-profile <profile-name>
```

```

assoc-boost
basic-rates-6ghz {12|18|24|36|48|54|6|9}
beacon-period <beacon-period>
beacon-rate-6ghz {12|18|24|36|48|54|6|9|default}
cap-reg-eirp <cap-reg-eirp>
channel <channel>
clone <source>
csa
csa-count <csa-count>
deploy-hour
disable-arm-wids-functions {Dynamic | OFF | ON}
disable-probe-retry-6ghz
dot11h
dynamic-frag-level-6ghz {Level-0 | Level-1 | Level-2 | Level-3}
eirp-max
eirp-min
eirp-offset
frame-bursting-mode <dynamic|OFF|ON>
he-duration-based-rts-6ghz <he-duration-based-rts-6ghz>
he-guard-interval-6ghz {1600ns | 3200ns | 800ns}
he-mu-mimo-6ghz
he-mu-ofdma-6ghz
he-supported-mcs-map-6ghz <he-supported-mcs-map-6ghz>
he-txbf-6ghz
he-ul-mu-mimo-6ghz
ht-radio-profile <profile-name>
individual-twt-6ghz
max-channel-bandwidth
max-mpdu-size-6ghz
max-rx-a-mpdu-size-6ghz {16383|32767|65535|8191}
max-tx-a-mpdu-size-6ghz <max-tx-a-mpdu-size-6ghz>
max-vht-mpdu-size-6ghz {11454|3895|7991}
maximum-distance <maximum-distance>
mgmt-frame-throttle-interval <mgmt-frame-throttle-interval>
mgmt-frame-throttle-limit <mgmt-frame-throttle-limit>
min-mpdu-start-spacing-6ghz {.25|.5|0|1|16|2|4|8}
mode {am-mode | ap-mode | spectrum-mode}
no
rts-mode <always-disable|always-enable|default>
radio-enable
spectrum-monitoring
spectrum-profile <profile-name>
tx-power <tx-power>
tx-rates-6ghz {12|18|24|36|48|54|6|9}

```

Description

This command configures the radio settings for a 802.11 6 GHz radio profile in the applicable access points. Each 6 GHz radio profile includes a reference to an ARM profile, high-throughput radio profile, and RRM IE radio profile. Channels must be valid for the country configured in the AP regulatory domain profile (see [ap regulatory-domain-profile on page 341](#)). To view the supported channels, use the `show ap allowed-channels` command.

Parameter	Description
6ghz-advertise-ap-name	Allows the 6 GHz radios, which are part of the virtual AP, to broadcast the AP name information in the beacon frames.
6ghz-dot11k-enable	Enables 802.11k capability for 6 GHz radio.
6ghz-mbo-enable	Enables Agile Multiband (MBO) for 6 GHz radio. Also enables mfp-capable, 802.11k and 802.11u interworking implicitly on the AP.
6ghz-rrm-ie-profile <profile-name>	Configures a Radio Resource Management (RRM) Information Elements (IE) profile to define the information elements advertised by a Wi-Fi 6E AP for 6 GHz band.
advertise-location-6ghz	Enables all 6 GHz virtual APs to broadcast their GPS coordinates in the beacon and probe response frames.
am-scan-profile <profile-name>	Configures an Air Monitor (AM) scanning profile for the various channels on 6 GHz radio.
arm-profile <profile-name>	Configures an Adaptive Radio Management (ARM) profile that is applied to a radio profile for the 6 GHz frequency band.
assoc-boost	Increases the client association success rate, especially in a noisy environment. When this parameter is enabled: <ul style="list-style-type: none"> ■ The management frame retransmission retry limit in the radio

Parameter	Description
	<p>firmware for both authentication and association response is increased, thereby increasing the management frame retransmission rate.</p> <ul style="list-style-type: none"> ■ If the management frame retransmission retry limit is reached, another round of management frames are scheduled after a short time delay. ■ If a client starts an association (by sending a probe or authentication request), AP scanning is rejected for 5 seconds, thereby not missing the client association request.
<code>basic-rates-6ghz {12 18 24 36 48 54 6 9}</code>	<p>Selects the basic rates for 6 GHz radio. The available values are 6, 9, 12, 18, 24, 36, 48, 54.</p>
<code>beacon-period <beacon-period></code>	<p>Configures the beacon period for the AP in msec.</p> <p>Range: 60-1000 msec</p> <p>Default: 100 msec</p>
<code>beacon-rate-6ghz {12 18 24 36 48 54 6 9 default}</code>	<p>Configures the beacon rate for 6 GHz radio. (For Distributed Antenna System (DAS) only).</p> <p>Default: Minimum valid rate</p>
<code>cap-reg-eirp <cap-reg-eirp></code>	<p>Workaround to override reg maximum EIRP in dot11d for interoperability with misbehaving clients.</p>

Parameter	Description
channel <channel>	<p>Channel number for the Wi-Fi 6E AP on 6 GHz radio band. The available channels depend on the regulatory domain (country). This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface. Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes:</p> <ul style="list-style-type: none">▪ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel.▪ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel.▪ num-: Entering a channel number with

Parameter	Description
	<p>a minus (-) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel.</p> <p>NOTE: 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.</p>
clone <source>	Name of an existing radio profile from which parameter values are copied.
csa	<p>Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel.</p> <p>Clients must support CSA in order to track the channel change without experiencing disruption.</p>

Parameter	Description
<code>csa-count <csa-count></code>	<p>Number of CSA announcements that are sent before the AP begins transmitting on the new channel.</p> <p>Range: 1-16</p> <p>Default: 4</p>
<code>deploy-hour</code>	<p>Configure hour-of-day for AP solution deployment. Overrides Airmatch profile if a valid hour is specified.</p> <p>Range: 0-23</p>
<code>disable-arm-wids-functions {Dynamic OFF ON}</code>	<p>Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option.</p> <p>CAUTION: Use carefully, since this effectively disables ARM and WIDS.</p>
<code>disable-probe-retry-6ghz</code>	<p>Enables or disables battery MAC level retries for probe response frames.</p>
<code>dot11h</code>	<p>Enables advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities</p>
<code>dynamic-frag-level-6ghz {Level-0 Level-1 Level-2 Level-3}</code>	<p>Configures the dynamic fragmentation level supported by the Wi-Fi 6E AP(only configurable in Bridge or D-tunnel mode):</p>

Parameter	Description
	<ul style="list-style-type: none"> ■ Level-0—Does not support dynamic fragmentation ■ Level-1—Supports dynamic fragments that are contained within a S-MPDU. Does not provide support for dynamic fragments within an A-MPDU that is not a S-MPDU. ■ Level-2—Supports dynamic fragments that are contained within a S-MPDU and support for up to one dynamic fragment for each MSDU within an A-MPDU. ■ Level-3—Supports dynamic fragments that are contained within a S-MPDU and support for up to four dynamic fragment for each MSDU within an A-MPDU. <p>Default: Level-0</p> <p>NOTE: This parameter is further limited by each AP's radio hardware capabilities.</p>
eirp-max	<p>Maximum EIRP. Further limited by regulatory domain constraints and AP capabilities.</p> <p>Range: 1 - 127</p>
eirp-min	<p>Minimum EIRP.</p> <p>Range: 1 - 127</p>
eirp-offset	<p>User offset of EIRP on top of algorithm choice.</p> <p>Range: Integer in [-6,6]</p> <p>Default: 0 dB</p>

Parameter	Description
<pre>frame-bursting-mode</pre>	<p>In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference where the traffic of an active client could affect the air traffic of neighboring APs within the same channel. Starting from ArubaOS 8.11.0.0, users are allowed to control frame bursting even if there's only one active client associated to the AP.</p> <ul style="list-style-type: none"> ■ Dynamic: Frame bursting will be enabled only when one active client is connected to the AP, and frame bursting will be disabled when there is more than one active client. ■ OFF: Frame bursting mode is always disabled. ■ ON: Frame bursting mode is always enabled.
<pre>he-duration-based-rts-6ghz <he-duration-based-rts-6ghz></pre>	<p>Indicates HE duration-based RTS value. When the TXOP is greater than the configured HE duration based RTS value, RTS/CTS exchange should be used. Range: 0-1023(units: 32ms).</p> <p>Default: 1023 1023: HE duration-based RTS will be disabled.</p>
<pre>he-guard-interval-6ghz {1600ns 3200ns 800ns}</pre>	<p>Enables or disables supported HE guard intervals.</p> <p>Default: All enabled</p>

Parameter	Description
he-mu-mimo-6ghz	Enables or disables HE MU-MIMO. (802.11ax APs only). Default: enabled
he-mu-ofdma-6ghz	Enables or disables HE MU-OFDMA. (802.11ax APs only). Default: enabled
he-supported-mcs-map-6ghz <he-supported-mcs-map-6ghz>	Comma list of max supported MCS for spatial streams 1 through 8. Valid values for max mcs are 7, 9, 11 and '-' ('-' means spatial stream is not supported, and it's not supported at first spatial stream). Max mcs of a spatial stream cannot be higher than the previous stream's. If a MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx. Default: 11,11,11,11,11,11,11,11
he-txbf-6ghz	Enables or disables HE TXBF. Default: enabled
he-ul-mu-mimo-6ghz	Enables or disables HE UL MU-MIMO. Default: disabled
ht-radio-profile <profile-name>	Configures high-throughput radio profile.
individual-twt-6ghz	Enables or disables Individual TWT support. Default: enabled

Parameter	Description
max-channel-bandwidth	Maximum channel bandwidth in MHz. Valid values are 20MHz, 40MHz, 80MHz and 160MHz. 80MHz and above is not allowed for dot11g-radio-profile.
max-mpdu-size-6ghz	Maximum size of an MPDU. Permitted values: 3895, 7991, 11454. Default: 11454
max-rx-a-mpdu-size-6ghz	Configures maximum size of a received aggregate MPDU. Allowed values are 8191, 16383, 32767, and 65535.
max-tx-a-mpdu-size-6ghz	Configures maximum size of a transmitted aggregate MPDU. Range: 1576-65535
max-vht-mpdu-size-6ghz	Configures maximum size of a VHT MPDU. Allowed values are 3895, 7991, and 11454. Default: 11454
maximum-distance	Configures maximum wireless-link distance [meters]. Used to derive slot-time and ACK and CTS timeouts.

Parameter	Description
	<p>0 means use defaults: timeouts are unmodified except for outdoor mesh-radios which use 16km. Upper limits: legacy/11N AP 20MHz: 52km; 11N AP 40MHz: 24km; 11AC AP: 48km. Values above maximum supported cause the maximum to be used, below 600m defaults are used. Outdoor mesh points start up with the maximum supported until configured.</p>
<pre>mgmt-frame-throttle-interval <mgmt-frame-throttle-interval></pre>	<p>Averaging interval for rate limiting mgmt frames from this radio in secs. 0 disables rate limiting.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p>
<pre>mgmt-frame-throttle-limit <mgmt-frame-throttle-limit></pre>	<p>Maximum number of mgmt frames that can come in from this radio in each throttle interval.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p>
<pre>min-mpdu-start-spacing-6ghz { .25 .5 0 1 16 2 4 8 }</pre>	<p>Minimum time between the start of adjacent subframes within an aggregate MPDU. Due to hardware differences, on some platforms this value will be silently restricted to 8us even if a lower value is configured.</p>
<pre>mode</pre>	<p>One of the operating modes for the AP.</p>

Parameter	Description
	Default: ap-mode
ap-mode	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.
am-mode	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
spectrum-mode	Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.
no	Negates any configured parameter.
radio-enable	Enables or disables radio configuration. Default: enabled
rts-mode	<p>RTS mode allows users to control RTS frame transmission to the clients.</p> <ul style="list-style-type: none"> ■ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ■ always-disable: RTS is not used for any transmission. ■ default: The

Parameter	Description
	<p>default RTS mode configured in the wireless driver of the AP is used. For 300 Series, 310 Series, 360 Series, 370 Series, AP-387, 530 Series, AP-555, 580 Series, 630 Series, and 635 Series access points, RTS is used for every alternate retried PPDU transmission. For 500H Series, 500 Series, 510 Series, 560 Series, 570 Series, 610 Series access points, RTS is used for all AMPDU transmissions.</p> <p>default</p>
spectrum-load-balancing	<p>The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.</p> <p>Default: disabled</p>

Parameter	Description
<p>spectrum-monitoring</p>	<p>This parameter turns APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.</p> <p>For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide.</p> <p>For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.</p> <p>default</p>
<p>spectrum-profile <profile></p>	<p>Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 1254.</p>
<p>tx-power <tx-power></p>	<p>Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration.</p> <p>This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm.</p>

Parameter	Description
	<p>Transmission power may be further limited by regulatory domain constraints and AP capabilities.</p> <p>NOTE: This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface.</p> <p>Range: -51 dBm to 51 dBm</p> <p>Default: 14 dBm</p>
<code>tx-rates-6ghz {12 18 24 36 48 54 6 9}</code>	<p>Sets the transmit rates for 6 GHz radio. The available values are 6, 9, 12, 18, 24, 36, 48, 54.</p>

Example

The following command enables the Agile Multiband Operation (MBO) for a 6 GHz radio profile "rf-6-635".

```
(host)[mynode](config)#rf dot11-6gHz-radio-profile rf-6-635
(host)[mynode] (6GHz radio profile "rf-6-635") #6ghz-dot11k-enable
(host)[mynode] (6GHz radio profile "rf-6-635") #6ghz-mbo-enable
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The frame-bursting-mode and rts-mode parameters were introduced.
ArubaOS 8.9.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf dot11a-radio-profile

```
rf dot11a-radio-profile <profile>
  am-scan-profile <profile-name>
  am-tx-mute
  arm-profile <profile>
  assoc-boost
  beacon-period <milliseconds>
  beacon-regulate
  cap-reg-eirp <cap-reg-eirp>
  cell-size-reduction <cell-size-reduction>
  channel <num|num+|num->
  channel-reuse {static|dynamic|disable}
  channel-reuse-threshold
  clone <profile>
  csa
  csa-count <number>
  deploy-hour <deploy-hour>
  disable-arm-wids-functions
  dot11h
  eirp-max <eirp-max>
  eirp-min <eirp-min>
  eirp-offset <eirp-offset>
  energy-detect-threshold <energy-detect-threshold>
  frame-bursting-mode <dynamic|OFF|ON>
  high-efficiency-enable <radio>
  high-throughput-enable
  ht-radio-profile <profile>
  interference-immunity
  max-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  maximum-distance <maximum-distance>
  mgmt-frame-throttle-interval <seconds>
  mgmt-frame-throttle-limit <number>
  min-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  min-mpdu-start-spacing-6Ghz
  mode {ap-mode|am-mode|spectrum-mode}
  no ...
  radar-test-mode
  radio-enable
  rts-mode <always-disable|always-enable|default>
  slb-mode channel|radio
  slb-threshold
  slb-update-interval <secs>
  spectrum-load-bal-domain
  spectrum-load-balancing
  spectrum-monitoring
  spectrum-profile <profile>
  spur-immunity <spur-immunity>
  transmit
  tx-power <dBm>
  very-high-throughput-enable
  zero-wait-dfs
```


Description

This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile for standalone controllers and the high-throughput (802.11n) radio profile. Channels must be valid for the country configured in the AP regulatory domain profile (see [ap regulatory-domain-profile on page 341](#)). To view the supported channels, use the `show ap allowed-channels` command.

APs initially start up with default **ack-timeout**, **cts-timeout** and **slot-time** values. When you modify the `maximum-distance` parameter in an `rf dot11a` radio profile or `rf dot11g` radio profile, new **ack-timeout**, **cts-timeout** and **slot-time** values may be derived, but those values are never less than the default values for an indoor AP.

Mesh radios on outdoor APs have additional constraints, as mesh links may need to span long distances. For mesh radios on outdoor APs, the effect of the default `maximum-distance` parameter on the **ack-timeout**, **cts-timeout** and **slot-time** values depends on whether the APs are configured as mesh portals or mesh points. This is because mesh portals use a default **maximum-distance** value of 16,050 meters, and mesh points use, by default, the maximum possible **maximum-distance** value.

The **maximum-distance** value should be set correctly to span the largest link distance in the mesh network so that when a mesh point gets the configuration from the network it will apply the correct **ack-timeout**, **cts-timeout** and **slot-time** values. The values derived from the **maximum-distance** setting depend on the band and whether 20MHz/40MHz mode of operation is in use.

The following table indicates values for a range of distances:

Timeouts[usec]	--- 5GHz radio ---			--- 2.4GHz radio ---		
Distance[m]	Ack	CTS	Slot	Ack	CTS	Slot
0 (outdoor:16050m)	128	128	63	128	128	63
0 (indoor:600a,6450g)	25	25	9	64	48	9
200 (==default)	25	25	9	64	48	9
500	25	25	9	64	48	9
600	25	25	9	64	48	9
1050	28	28	13	64	48	31
5100	55	55	26	64	55	31
10050	88	88	43	88	88	43
15000	121	121	59	121	121	59
16050	128	128	63	128	128	63
58200(5G limit 20M)	409	409	203	-	-	-
52650(2.4G limit 20M)	-	-	-	372	372	185
27450(5G limit 40M)	204	204	101	-	-	-
24750(2.4G limit 40M)	-	-	-	186	186	92

Parameter	Description
<profile>	Name of this instance of the profile. The name must be 1-63 characters. default
am-scan-profile <name>	Configure an Air Monitor (AM) scanning profile. default
arm-profile	Configures Adaptive Radio Management (ARM) feature. See rf arm-profile on page 1151 . default
am-tx-mute	Mute the radio transmission when in AM mode. Disabled
assoc-boost	The assoc-boost parameter increases the client association success rate, especially in a noisy environment. When this parameter is enabled: <ul style="list-style-type: none"> ▪ The management frame retransmission retry limit in the radio firmware for both authentication and association response is increased, thereby increasing the management frame retransmission rate. ▪ If the management frame retransmission retry limit is reached, after a short time delay another round of management frames are scheduled. ▪ If a client starts an association (by sending a probe or authentication request), AP scanning is rejected for 5 seconds, thereby not missing the client association request. disabled
beacon-period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients. 60 (minimum) 100 milli-seconds
beacon-regulate	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. disabled

Parameter	Description
<pre>cap-reg-eirp <cap-reg-eirp></pre>	<p>Work around a known issue on Cisco 7921G telephones by specifying a cap for a radio's maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.</p> <p>1–31 dBm</p>
<pre>cell-size-reduction <cell-size-reduction></pre>	<p>The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issues. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.</p> <p>Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.</p> <p>1-55dB</p> <p>0 dB</p>
<pre>channel</pre>	<p>Channel number for the AP 802.11a/802.11n/802.11ac physical layer. This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface.</p> <p>The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes:</p> <ul style="list-style-type: none"> ▪ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ▪ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ▪ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary

Parameter	Description
	<p>channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel.</p> <p>NOTE: 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.</p> <p>Depends on regulatory domain</p>
channel-reuse	<p>When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.)</p> <ul style="list-style-type: none"> ▪ Static mode: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ▪ Dynamic mode: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ▪ Disable mode: This mode does not support the tuning of the CCA Detect Threshold. <p>enabled, disabled enabled</p>
channel-reuse-threshold	<p>RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm.</p> <p>If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength.</p> <p>If the value is set to zero, the feature will automatically determine an appropriate threshold.</p> <p>Depends on regulatory domain</p>
clone	<p>Name of an existing radio profile from which parameter values are copied.</p>

Parameter	Description
csa	<p>Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.</p> <p>disabled</p>
csa-count	<p>Number of CSA announcements that are sent before the AP begins transmitting on the new channel.</p> <p>1-16</p> <p>4</p>
deploy-hour <0-23>	<p>Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.</p> <p>0-23</p> <p>5</p>
disable-arm-wids-functions	<p>Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option.</p> <p>CAUTION: Use carefully, since this effectively disables ARM and WIDS.</p> <p>disabled</p>
dot11h	<p>Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities.</p> <p>disabled</p>
eirp-max <eirp-max>	<p>Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p>

Parameter	Description
	1-127 18
<code>eirp-min <eirp-min></code>	<p>The minimum transmission power level (in dBm) to be assigned to the AP radio(s).</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> 1-127 12
<code>eirp-offset</code>	<p>Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> -6 to 6 dBm 0 dBm
<code>energy-detect-threshold</code>	<p>Modify the Energy Detect Threshold (EDT) used by the radio in making transmit decisions. The EDT is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. Specify a value of 0 to use the default EDT for this radio. (This value may vary by AP model)</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> 0, 1-12 0 (disabled) Starting from ArubaOS 8.7.1.1, the range of <code>energy-detect-threshold</code> parameter has been modified from 0-12 to 12 to -29 dB.
<code>frame-bursting-mode</code>	<p>In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference where the traffic of an active client could affect the air traffic of neighboring APs within the same channel. Starting from ArubaOS 8.11.0.0, users are allowed to control frame bursting even if there's only one active client associated to the AP.</p> <ul style="list-style-type: none"> Dynamic: Frame bursting will be enabled only when

Parameter	Description
	<p>one active client is connected to the AP, and frame bursting will be disabled when there is more than one active client.</p> <ul style="list-style-type: none"> ■ OFF: Frame bursting mode is always disabled. ■ ON: Frame bursting mode is always enabled.
high-efficiency-enable <radio>	<p>Enables high-efficiency (802.11ax) features on a radio by using the 5 GHz frequency band.</p> <p>enabled</p>
high-throughput-enable	<p>Enables high-throughput (802.11n) features on a radio using the 5 GHz frequency band.</p> <p>enabled</p>
ht-radio-profile	<p>Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See rf ht-radio-profile on page 1249.</p> <p>default-a</p>
interference-immunity	<p>Set a value for 802.11 interference immunity. This parameter sets the interference immunity on the 5 GHz band. When performance drops due to interference from non- 802.11 interferers (such as DECT or Bluetooth devices), the level can be increased for improved performance. There are 17 levels (0-16) and Table 8 lists the settings applied for each level.</p> <p>NOTE: It is recommended not to adjust interference immunity without guidance from Aruba support. Increasing the immunity level in a healthy network may result in severe loss of performance. This should be set to a higher than default level only when there is significant degradation due to non-Wi-Fi interference.</p> <p>0-16 2</p>
max-channel-bandwidth	<p>Sets the maximum channel bandwidth for APs associated to Mobility Conductor managed devices.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>20MHz, 40MHz, 80MHz or 160MHz 80MHz</p>
minimum-channel-bandwidth	<p>Sets the minimum channel bandwidth for APs associated to Mobility Conductor managed devices.</p>

Parameter	Description
	<p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>20MHz, 40MHz, 80MHz 20MHz</p>
min-mpdu-start-spacing-6Ghz	Sets the minimum time between the start of adjacent subframes within an aggregate MPDU. Due to hardware differences, on some platforms this value will be silently restricted to 8us even if a lower value is configured.
maximum-distance	<p>Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.</p> <p>The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 5 GHz frequency band radio:</p> <ul style="list-style-type: none"> ▪ 20MHz mode: 58km ▪ 40MHz mode: 27km <p>Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.</p> <p>0-57km (40MHz mode), 0-27km (20MHz mode) 0 meters</p>
mgmt-frame-throttle-interval	<p>Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-60 1 second interval</p>
mgmt-frame-throttle-limit	<p>Maximum number of management frames allowed in each throttle interval.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-999999 20 frames per interval</p>
mode	<p>One of the operating modes for the AP.</p> <p>ap-mode</p>

Parameter	Description
ap-mode	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.
am-mode	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
spectrum-mode	Device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
no	Negates any configured parameter.
radar-test-mode	For internal use only.
radio-enable	Enables or disables radio configuration. enabled
rts-mode	RTS mode allows users to control RTS frame transmission to the clients. <ul style="list-style-type: none"> ■ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ■ always-disable: RTS is not used for any transmission. ■ default: The default RTS mode configured in the wireless driver of the AP is used. For 300 Series, 310 Series, 360 Series, 370 Series, AP-387, 530 Series, AP-555, 580 Series, 630 Series, and 635 Series access points, RTS is used for every alternate retried PPDU transmission. For 500H Series, 500 Series, 510 Series, 560 Series, 570 Series, 610 Series access points, RTS is used for all AMPDU transmissions. default
slb-mode channel radio	SLB Mode allows control over how to balance clients. Select one of the following options <ul style="list-style-type: none"> ■ channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ radio: Radio-based load-balancing balances clients across APs channel
slb-update-interval <secs>	Specify how often spectrum load balancing calculations are made (in seconds). 1-2147483647 seconds 30 seconds
smart-antenna	Enable or disable the smart antenna feature on AP-335 access points. enabled, disabled

Parameter	Description
	enabled
spectrum-load-bal -domain	<p>Define a spectrum load balancing domain to manually create RF neighborhoods.</p> <p>Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment.</p> <ul style="list-style-type: none"> ▪ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is not defined, ArubaOS uses ARM to calculate RF neighborhoods. ▪ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain is also defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.
spectrum-load- balancing	<p>The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.</p> <p>disabled</p>
spectrum-monitoring	<p>Issue this command to turn APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.</p> <p>For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide.</p> <p>For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.</p> <p>default</p>
spectrum-profile <profile>	<p>Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 1254.</p> <p>default</p>

Parameter	Description
<code>spur-immunity <spur-immunity></code>	<p>Spur Immunity for 5 GHz radio. This parameter fine-tunes the Cyclic Power Threshold (CPT) of a 5 GHz radio. The value specified here is the offset from the base value of 2 dB (for example, setting the CPT value to 1 corresponds to 2 + 1 = 3 dB. Similarly, setting the CPT value to 10 corresponds to 2+10 = 12 dB).</p> <p>Use this parameter when high channel utilization is observed in the 5 GHz radio of 130 Series access points in a noise-free environment causing client association or throughput issues.</p> <p>Adjust the CPT value to eliminate the spur impacts. Range definition is as follows:</p> <ul style="list-style-type: none"> ▪ 0: default CPT ▪ 1-19: CPT growth from default (3 dB to 21 dB) ▪ 20: Setting this parameter to 20 sets the cell-size-reduction value to 1. Cell-size-reduction is the receive coverage area of the AP. <p>NOTE: Configure this parameter under the supervision of Aruba Technical Support.</p> <p>NOTE: Setting the spur immunity to a higher value may decrease the AP RF coverage.</p> <p>NOTE: This parameter is applicable for 130 Series access points only. The controller ignores this parameter if configured for non-130 Series access points.</p> <p>0-20 CPT 0 CPT</p>
<code>transmit</code>	<p>Enable or disable transmission of frames on the radio.</p> <p>NOTE: This parameter should only be used for radio test purposes.</p> <p>enabled, disabled disabled</p>
<code>tx-power</code>	<p>Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration. This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface. This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities.</p>

Parameter	Description
	<p>NOTE: Use this parameter to set transmit power levels for APs associated to a stand-alone controller not using ARM.</p> <p>-51 dBm to 51 dBm 14 dBm</p>
very-high-throughput-enable	<p>Enable or disable support for Very High Throughput (802.11ac) on the radio.</p> <p>Enabled</p>
zero-wait-dfs	<p>Enable or disable support for zero-wait DFS channel feature. This feature provides seamless change of channels and avoids the period of no transmission. Hence, stations do not lose their connectivity when an AP moves to a DFS channel.</p> <p>Default: Disabled</p> <p>NOTE: All 510 Series, 518 Series, 530 Series, 550 Series, 570 Series, 580 Series, and 650 Series access points having 4x4 5 GHz radios support the zero-wait DFS feature.</p>

Examples

The following command configures APs to operate in AM mode for the selected dot11a-radio-profile named "sample-a:"

```
(host) [node] (config) #rf dot11a-radio-profile sample-a mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 5 GHz frequency band for the selected dot11a-radio profile named "sample-a-" and assigns a high-throughput radio profile named "default-a:"

```
(host) [node] (config) #rf dot11a-radio-profile sample-a
high-throughput-enable
ht-radio-profile default-a
```

The following command configures a primary channel number of 157 and a secondary channel number of 161 for 40 MHz mode of operation with a dot11a-radio profile named "sample-a:"

```
(host) [node] (config) #rf dot11a-radio-profile sample-a channel <157+>
```

The following table indicates the interference immunity implementation for each level.

Table 8: Interference Immunity Levels

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
0	Disabled	Disabled	Enabled	None	None
1	Enabled	Disabled	Enabled	None	None
2	Enabled	Enabled	Enabled	None	None
3	Enabled	Enabled	Enabled	None	None
4	Enabled	Enabled	Enabled	4 dB	None
5	Enabled	Enabled	Enabled	8 dB	None
6	Enabled	Enabled	Enabled	12 dB	None
7	Enabled	Enabled	Enabled	16 dB	None
8	Enabled	Enabled	Enabled	None	-85 dB
9	Enabled	Enabled	Enabled	None	-80 dB
10	Enabled	Enabled	Enabled	None	-75 dB
11	Enabled	Enabled	Enabled	8 dB	-85 dB
12	Enabled	Enabled	Enabled	8 dB	-80 dB
13	Enabled	Enabled	Enabled	None	None
14	Enabled	Enabled	Enabled	None	None
15	Enabled	Enabled	Enabled	8 dB	None
16	Enabled	Enabled	Enabled	16 dB	None

- **Adaptive Noise Immunity:** Adjust noise and spur immunity levels based on PHY errors.
- **Preemption mode:** The radio stops current reception and restarts the receiver when a new signal which is above the threshold of the current signal is found. This allows the radio to switch signals when it locks onto interference or weaker 802.11 signal, when a valid 802.11 signal with a higher signal strength is detected.
- **Low Noise Amplifier:** Enables radio saturation at lower signal levels resulting in better performance in the presence of interference. Disabling LNA avoids radio saturation at lower signal levels. However, it may reduce range and throughput.

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
<ul style="list-style-type: none"> ▪ Interference Sensitivity Reduction: Reduces the sensitivity to both Wi-Fi and non Wi-Fi interference signals. This makes the radio deaf to signals in which the SNR is below the threshold. ▪ Force Noise Floor (for 2.4 GHz radio only): Forces the radio to use the configured value as the absolute noise floor value. This makes the radio ignore signals of weaker amplitude. 					

Command History

Release	Modification
ArubaOS 8.11.0.0	The frame-bursting-mode and rts-mode parameters were introduced.
ArubaOS 8.8.0.0	The <code>zero-wait-dfs</code> parameter was introduced.
ArubaOS 8.7.1.1	The range of <code>energy-detect-threshold</code> parameter has been modified from 0-12 to 12 to -29 dB.
ArubaOS 8.4.0.0	The <code>high-efficiency-enable <radio></code> parameter was added.
ArubaOS 8.2.0.0	Modified the range of the <code>eirp-max</code> and <code>eirp-min</code> parameters.
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none"> ▪ <code>deploy-hour</code>, <code>eirp-offset</code> ▪ <code>energy-detect-threshold</code> ▪ <code>minimum-channel-bandwidth</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Config mode on Mobility Conductor.

rf dot11a-secondary-radio-profile

```
rf dot11a-secondary-radio-profile <profile>
  am-scan-profile <profile-name>
  arm-profile <profile>
  beacon-period <milliseconds>
  beacon-regulate
  cap-reg-eirp <cap-reg-eirp>
  cell-size-reduction <cell-size-reduction>
  channel <num|num+|num->
  channel-reuse {static|dynamic|disable}
  channel-reuse-threshold
  clone <profile>
  csa
  csa-count <number>
  deploy-hour <deploy-hour>
  disable-arm-wids-functions
  dot11h
  eirp-max <eirp-max>
  eirp-min <eirp-min>
  eirp-offset <eirp-offset>
  energy-detect-threshold <energy-detect-threshold>
  frame-bursting-mode <dynamic|OFF|ON>
  high-efficiency-enable <radio>
  high-throughput-enable
  ht-radio-profile <profile>
  interference-immunity
  max-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  maximum-distance <maximum-distance>
  mgmt-frame-throttle-interval <seconds>
  mgmt-frame-throttle-limit <number>
  min-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  mode {ap-mode|am-mode|spectrum-mode}
  no ...
  radar-test-mode
  radio-enable
  rts-mode <always-disable|always-enable|default>
  slb-mode channel|radio
  slb-threshold
  slb-update-interval <secs>
  spectrum-load-bal-domain
  spectrum-load-balancing
  spectrum-monitoring
  spectrum-profile <profile>
  spur-immunity <spur-immunity>
  transmit
  tx-power <dBm>
  very-high-throughput-enable
  zero-wait-dfs
```

Description

This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile for standalone controllers and the high-throughput (802.11n) radio profile. Channels must be valid for the country configured in the AP regulatory domain profile (see [ap regulatory-domain-profile on page 341](#)). To view the supported channels, use the `show ap allowed-channels` command.

APs initially start up with default **ack-timeout**, **cts-timeout** and **slot-time** values. When you modify the `maximum-distance` parameter in an `rf dot11a` radio profile or `rf dot11g` radio profile, new **ack-timeout**, **cts-timeout** and **slot-time** values may be derived, but those values are never less than the default values for an indoor AP.

Mesh radios on outdoor APs have additional constraints, as mesh links may need to span long distances. For mesh radios on outdoor APs, the effect of the default `maximum-distance` parameter on the **ack-timeout**, **cts-timeout** and **slot-time** values depends on whether the APs are configured as mesh portals or mesh points. This is because mesh portals use a default **maximum-distance** value of 16,050 meters, and mesh points use, by default, the maximum possible **maximum-distance** value.

The **maximum-distance** value should be set correctly to span the largest link distance in the mesh network so that when a mesh point gets the configuration from the network it will apply the correct **ack-timeout**, **cts-timeout** and **slot-time** values. The values derived from the **maximum-distance** setting depend on the band and whether 20MHz/40MHz mode of operation is in use.

The following table indicates values for a range of distances:

Timeouts[usec]	--- 5GHz radio ---			--- 2.4GHz radio ---		
Distance[m]	Ack	CTS	Slot	Ack	CTS	Slot
0 (outdoor:16050m)	128	128	63	128	128	63
0 (indoor:600a,6450g)	25	25	9	64	48	9
200 (==default)	25	25	9	64	48	9
500	25	25	9	64	48	9
600	25	25	9	64	48	9
1050	28	28	13	64	48	31
5100	55	55	26	64	55	31
10050	88	88	43	88	88	43
15000	121	121	59	121	121	59
16050	128	128	63	128	128	63
58200(5G limit 20M)	409	409	203	-	-	-
52650(2.4G limit 20M)	-	-	-	372	372	185
27450(5G limit 40M)	204	204	101	-	-	-
24750(2.4G limit 40M)	-	-	-	186	186	92

Parameter	Description
<profile>	Name of this instance of the profile. The name must be 1-63 characters. default

Parameter	Description
am-scan-profile <name>	Configure an Air Monitor (AM) scanning profile. default
arm-profile	Configures Adaptive Radio Management (ARM) feature. See rf arm-profile on page 1151 . default
assoc-boost	<p>The assoc-boost parameter increases the client association success rate, especially in a noisy environment. When this parameter is enabled:</p> <ul style="list-style-type: none"> ▪ The management frame retransmission retry limit in the radio firmware for both authentication and association response is increased, thereby increasing the management frame retransmission rate. ▪ If the management frame retransmission retry limit is reached, after a short time delay another round of management frames are scheduled. ▪ If a client starts an association (by sending a probe or authentication request), AP scanning is rejected for 5 seconds, thereby not missing the client association request. <p>disabled</p>
beacon-period	<p>Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.</p> <p>60 (minimum) 100 milli-seconds</p>
beacon-regulate	<p>Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.</p> <p>disabled</p>
cap-reg-eirp <cap-reg-eirp>	<p>Work around a known issue on Cisco 7921G telephones by specifying a cap for a radio's maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.</p> <p>1–31 dBm</p>

Parameter	Description
<p>cell-size-reduction <cell-size-reduction></p>	<p>The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issues. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.</p> <p>Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.</p> <p>1-55dB 0 dB</p>
<p>channel</p>	<p>Channel number for the AP 802.11a/802.11n/802.11ac physical layer. This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface.</p> <p>The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes:</p> <ul style="list-style-type: none"> ▪ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ▪ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ▪ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel. <p>NOTE: 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.</p> <p>Depends on regulatory domain</p>

Parameter	Description
channel-reuse	<p>When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.)</p> <ul style="list-style-type: none"> ■ Static mode: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ Dynamic mode: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ Disable mode: This mode does not support the tuning of the CCA Detect Threshold. <p>enabled, disabled enabled</p>
channel-reuse-threshold	<p>RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm.</p> <p>If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength.</p> <p>If the value is set to zero, the feature will automatically determine an appropriate threshold.</p> <p>Depends on regulatory domain</p>
clone	<p>Name of an existing radio profile from which parameter values are copied.</p>
csa	<p>Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.</p> <p>disabled</p>
csa-count	<p>Number of CSA announcements that are sent before the AP begins transmitting on the new channel.</p>

Parameter	Description
	1-16 4
<code>deploy-hour <0-23></code>	<p>Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.</p> 0-23 5
<code>disable-arm-wids-functions</code>	<p>Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option.</p> <p>CAUTION: Use carefully, since this effectively disables ARM and WIDS.</p> disabled
<code>dot11h</code>	<p>Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities.</p> disabled
<code>eirp-max <eirp-max></code>	<p>Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> 1-127 18
<code>eirp-min <eirp-min></code>	<p>The minimum transmission power level (in dBm) to be assigned to the AP radio(s).</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone</p>

Parameter	Description
	<p>controller.</p> <p>1-127</p> <p>12</p>
eirp-offset	<p>Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>-6 to 6 dBm</p> <p>0 dBm</p>
energy-detect-threshold	<p>Modify the Energy Detect Threshold (EDT) used by the radio in making transmit decisions. The EDT is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. Specify a value of 0 to use the default EDT for this radio. (This value may vary by AP model)</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>0, 1-12</p> <p>0 (disabled)</p> <p>Starting from ArubaOS 8.7.1.1, the range of <code>energy-detect-threshold</code> parameter has been modified from 0-12 to 12 to -29 dB.</p>
frame-bursting-mode	<p>In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference where the traffic of an active client could affect the air traffic of neighboring APs within the same channel. Starting from ArubaOS 8.11.0.0, users are allowed to control frame bursting even if there's only one active client associated to the AP.</p> <ul style="list-style-type: none"> ■ Dynamic: Frame bursting will be enabled only when one active client is connected to the AP, and frame bursting will be disabled when there is more than one active client. ■ OFF: Frame bursting mode is always disabled. ■ ON: Frame bursting mode is always enabled.
high-efficiency-enable <radio>	<p>Enables high-efficiency (802.11ax) features on a radio by using the 5 GHz frequency band.</p>

Parameter	Description
	enabled
high-throughput-enable	Enables high-throughput (802.11n) features on a radio using the 5 GHz frequency band. enabled
ht-radio-profile	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See rf ht-radio-profile on page 1249 . default-a
interference-immunity	Set a value for 802.11 interference immunity. This parameter sets the interference immunity on the secondary 5 GHz band. When performance drops due to interference from non- 802.11 interferers (such as DECT or Bluetooth devices), the level can be increased for improved performance. There are 17 levels (0-16) and Table 9 lists the settings applied for each level. NOTE: It is recommended not to adjust interference immunity without guidance from Aruba support. 0-16 2
max-channel-bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Conductor managed devices. NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. 20MHz, 40MHz, 80MHz or 160MHz 80MHz
minimum-channel-bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Conductor managed devices. NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. 20MHz, 40MHz, 80MHz 20MHz

Parameter	Description
maximum-distance	<p>Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km.</p> <p>The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 5 GHz frequency band radio:</p> <ul style="list-style-type: none"> ▪ 20MHz mode: 58km ▪ 40MHz mode: 27km <p>Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.</p> <p>0-57km (40MHz mode), 0-27km (20MHz mode)</p> <p>0 meters</p>
mgmt-frame-throttle-interval	<p>Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-60</p> <p>1 second interval</p>
mgmt-frame-throttle-limit	<p>Maximum number of management frames allowed in each throttle interval.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-999999</p> <p>20 frames per interval</p>
mode	<p>One of the operating modes for the AP.</p> <p>ap-mode</p>
ap-mode	<p>Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.</p>
am-mode	<p>Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.</p>
spectrum-mode	<p>Device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.</p>
no	<p>Negates any configured parameter.</p>

Parameter	Description
radar-test-mode	For internal use only.
radio-enable	Enables or disables radio configuration. enabled
rts-mode	RTS mode allows users to control RTS frame transmission to the clients. <ul style="list-style-type: none"> ■ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ■ always-disable: RTS is not used for any transmission. ■ default: The default RTS mode configured in the wireless driver of the AP is used. For 300 Series, 310 Series, 360 Series, 370 Series, AP-387, 530 Series, AP-555, 580 Series, 630 Series, and 635 Series access points, RTS is used for every alternate retried PPDU transmission. For 500H Series, 500 Series, 510 Series, 560 Series, 570 Series, 610 Series access points, RTS is used for all AMPDU transmissions. default
slb-mode channel radio	SLB Mode allows control over how to balance clients. Select one of the following options <ul style="list-style-type: none"> ■ channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ radio: Radio-based load-balancing balances clients across APs channel
slb-update-interval <secs>	Specify how often spectrum load balancing calculations are made (in seconds). 1-2147483647 seconds 30 seconds
smart-antenna	Enable or disable the smart antenna feature on AP-335 access points. enabled, disabled enabled
spectrum-load-bal -domain	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. <ul style="list-style-type: none"> ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is not defined, ArubaOS uses ARM to calculate RF neighborhoods.

Parameter	Description
	<ul style="list-style-type: none"> If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain is also defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.
<pre>spectrum-load-balancing</pre>	<p>The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.</p> <p>disabled</p>
<pre>spectrum-monitoring</pre>	<p>Issue this command to turn APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.</p> <p>For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide.</p> <p>For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.</p> <p>default</p>
<pre>spectrum-profile <profile></pre>	<p>Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 1254.</p> <p>default</p>
<pre>spur-immunity <spur-immunity></pre>	<p>Spur Immunity for 5 GHz radio. This parameter fine-tunes the Cyclic Power Threshold (CPT) of a 5 GHz radio. The value specified here is the offset from the base value of 2 dB (for example, setting the CPT value to 1 corresponds to 2 + 1 = 3 dB. Similarly, setting the CPT value to 10 corresponds to 2+10 = 12 dB).</p> <p>Use this parameter when high channel utilization is observed in the 5 GHz radio of 130 Series access points in a noise-free environment causing client association or throughput issues.</p> <p>Adjust the CPT value to eliminate the spur impacts. Range definition is as follows:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ 0: default CPT ▪ 1-19: CPT growth from default (3 dB to 21 dB) ▪ 20: Setting this parameter to 20 sets the cell-size-reduction value to 1. Cell-size-reduction is the receive coverage area of the AP. <p>NOTE: Configure this parameter under the supervision of Aruba Technical Support.</p> <p>NOTE: Setting the spur immunity to a higher value may decrease the AP RF coverage.</p> <p>NOTE: This parameter is applicable for 130 Series access points only. The controller ignores this parameter if configured for non-130 Series access points.</p> <p>0-20 CPT 0 CPT</p>
transmit	<p>Enable or disable transmission of frames on the radio.</p> <p>NOTE: This parameter should only be used for radio test purposes.</p> <p>enabled, disabled disabled</p>
tx-power	<p>Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration. This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface. This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities.</p> <p>NOTE: Use this parameter to set transmit power levels for APs associated to a stand-alone controller not using ARM.</p> <p>-51 dBm to 51 dBm 14 dBm</p>
very-high-throughput-enable	<p>Enable or disable support for Very High Throughput (802.11ac) on the radio.</p> <p>Enabled</p>

Parameter	Description
zero-wait-dfs	<p>Enable or disable support for zero-wait DFS channel feature. This feature provides seamless change of channels and avoids the period of no transmission. Hence, stations do not lose their connectivity when an AP moves to a DFS channel. Default: Disabled</p> <p>NOTE: All 500 Series, 500H Series, 510 Series, 530 Series, 550 Series, 560 Series, 570 Series, and 650 Series access points support the zero-wait DFS feature.</p>

Examples

The following command configures APs to operate in AM mode for the selected secondary dot11a-radio-profile named "sample-a:"

```
(host) [node] (config) #rf dot11a-secondary-radio-profile sample-a mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 5 Ghz frequency band for the selected secondary dot11a-radio profile named "samplea-" and assigns a high-throughput radio profile named "default-a:"

```
(host) [node] (config) #rf dot11a-secondary-radio-profile
sample-a
high-throughput-enable
ht-radio-profile default-a
```

The following command configures a primary channel number of 157 and a secondary channel number of 161 for 40 MHz mode of operation with a secondary dot11a-radio profile named "sample-a:"

```
(host) [node] (config) #rf dot11a-secondary-radio-profile sample-a channel
<157+>
```

Table 9: *Interference Immunity Levels*

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
0	Disabled	Disabled	Enabled	None	None

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
1	Enabled	Disabled	Enabled	None	None
2	Enabled	Enabled	Enabled	None	None
3	Enabled	Enabled	Enabled	None	None
4	Enabled	Enabled	Enabled	4 dB	None
5	Enabled	Enabled	Enabled	8 dB	None
6	Enabled	Enabled	Enabled	12 dB	None
7	Enabled	Enabled	Enabled	16 dB	None
8	Enabled	Enabled	Enabled	None	-85 dB
9	Enabled	Enabled	Enabled	None	-80 dB
10	Enabled	Enabled	Enabled	None	-75 dB
11	Enabled	Enabled	Enabled	8 dB	-85 dB
12	Enabled	Enabled	Enabled	8 dB	-80 dB
13	Enabled	Enabled	Enabled	None	None
14	Enabled	Enabled	Enabled	None	None
15	Enabled	Enabled	Enabled	8 dB	None
16	Enabled	Enabled	Enabled	16 dB	None

- **Adaptive Noise Immunity:** Adjust noise and spur immunity levels based on PHY errors.
- **Preemption mode:** The radio stops current reception and restarts the receiver when a new signal which is above the threshold of the current signal is found. This allows the radio to switch signals when it locks onto interference or weaker 802.11 signal, when a valid 802.11 signal with a higher signal strength is detected.
- **Low Noise Amplifier:** Enables radio saturation at lower signal levels resulting in better performance in the presence of interference. Disabling LNA avoids radio saturation at lower signal levels. However, it may reduce range and throughput.
- **Interference Sensitivity Reduction:** Reduces the sensitivity to both Wi-Fi and non Wi-Fi interference signals. This makes the radio deaf to signals in which the SNR is below the threshold.
- **Force Noise Floor (for 2.4 GHz radio only):** Forces the radio to use the configured value as the absolute noise floor value. This makes the radio ignore signals of weaker amplitude.

Command History

Release	Modification
ArubaOS 8.11.0.0	The frame-bursting-mode and rts-mode parameters were introduced.
ArubaOS 8.8.0.0	The <code>zero-wait-dfs</code> parameter was introduced.
ArubaOS 8.7.1.1	The range of <code>energy-detect-threshold</code> parameter has been modified from 0-12 to 12 to -29 dB.
ArubaOS 8.4.0.0	The <code>high-efficiency-enable <radio></code> parameter was added.
ArubaOS 8.2.0.0	Modified the range of the <code>eirp-max</code> and <code>eirp-min</code> parameters.
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none">▪ <code>deploy-hour</code>, <code>eirp-offset</code>▪ <code>energy-detect-threshold</code>▪ <code>minimum-channel-bandwidth</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Config mode on Mobility Conductor.

rf dot11-60GHz-radio-profile

```
rf dot11-60GHz-radio-profile <profile>
  channel
  clone
  no
```

Description

This command configures AP radio settings for the 60 GHz frequency band on a 802.11 60 GHz radio profile. Channels must be valid for the country configured in the AP regulatory domain profile (see [ap regulatory-domain-profile on page 341](#)). To view the supported channels, use the `show ap allowed-channels` command.

Parameter	Description
channel	Indicates the radio channel. Range: 0-3 Default: 2 NOTE: Channel 1 is not recommended due to EIRP limitations.
clone	Copies data from a different 802.11 60 GHz radio profile.
no	Disables the 802.11 60 GHz radio profile configuration.

Examples

The following command configures APs for the selected 802.11 60 GHz radio profile named "default".

```
(host) [mynode] (config) # rf dot11-60GHz-radio-profile default
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf dot11g-radio-profile

```
rf dot11g-radio-profile <profile>
  airmatch-mode-aware
  am-scan-profile <profile-name>
  am-tx-mute
  arm-profile <profile>
  assoc-boost
  beacon-period <milliseconds>
  beacon-regulate
  cap-reg-eirp <cap-reg-eirp>
  cell-size-reduction <cell-size-reduction>
  channel <num|num+|num->
  channel-reuse {static|dynamic|disable}
  channel-reuse-threshold
  clone <profile>
  csa
  csa-count <number>
  deploy-hour <deploy-hour>
  disable-arm-wids-functions
  dot11b-protection
  dot11h
  eirp-max 3|6|9|12|15|18|21|24|27|30|33|127
  eirp-min 3|6|9|12|15|18|21|24|27|30|33|127
  eirp-offset <eirp-offset>
  energy-detect-threshold <energy-detect-threshold>
  frame-bursting-mode <dynamic|OFF|ON>
  high-efficiency-enable <radio>
  high-throughput-enable
  ht-radio-profile <profile>
  interference-immunity
  iot-coex-enable
  max-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  maximum-distance <maximum-distance>
  mgmt-frame-throttle-interval <seconds>
  mgmt-frame-throttle-limit <number>
  min-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
  mode {ap-mode|am-mode|spectrum-mode}
  no ...
  radio-enable
  rts-mode <always-disable|always-enable|default>
  slb-mode channel|radio
  slb-threshold
  slb-update-interval <secs>
  smart-antenna
  spectrum-load-bal-domain
  spectrum-load-balancing
  spectrum-monitoring
  spectrum-profile
  transmit
  tx-power <dBm>
  very-high-throughput-enable
```


Description

This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile. Channels must be valid for the country configured in the AP regulatory domain profile (see [ap regulatory-domain-profile on page 341](#)). To view the supported channels, use the `show ap allowed-channels` command.

APs initially start up with default **ack-timeout**, **cts-timeout** and **slot-time** values. When you modify the `maximum-distance` parameter in an `rf dot11a` radio profile or `rf dot11g` radio profile, new **ack-timeout**, **cts-timeout** and **slot-time** values may be derived, but those values are never less than the default values for an indoor AP.

Mesh radios on outdoor APs have additional constraints, as mesh links may need to span long distances. For mesh radios on outdoor APs, the effect of the default `maximum-distance` parameter on the **ack-timeout**, **cts-timeout** and **slot-time** values depends on whether the APs are configured as mesh portals or mesh points. This is because mesh portals use a default **maximum-distance** value of 16,050 meters, and mesh points use, by default, the maximum possible **maximum-distance** value.

The **maximum-distance** value should be set correctly to span the largest link distance in the mesh network so that when a mesh point gets the configuration from the network it will apply the correct **ack-timeout**, **cts-timeout** and **slot-time** values. The values derived from the **maximum-distance** setting depend on the band and whether 20MHz/40MHz mode of operation is in use.

Parameter	Description
<code><profile></code>	Name of this instance of the profile. The name must be 1-63 characters. default
<code>airmatch-mode-aware</code>	If enabled, AirMatch turns off radios in high density deployment. Default: Disabled
<code>am-scan-profile <profile-name></code>	Configure an Air Monitor (AM) scanning profile.
<code>am-tx-mute</code>	Mute the radio transmission when in AM mode. Default: Disabled
<code>arm-profile</code>	Configures Adaptive Radio Management (ARM) feature. See rf arm-profile on page 1151 . default

Parameter	Description
assoc-boost	<p>The assoc-boost parameter increases the client association success rate, especially in a noisy environment. When this parameter is enabled:</p> <ul style="list-style-type: none"> ▪ The management frame retransmission retry limit in the radio firmware for both authentication and association response is increased, thereby increasing the management frame retransmission rate. ▪ If the management frame retransmission retry limit is reached, after a short time delay another round of management frames are scheduled. ▪ If a client starts an association (by sending a probe or authentication request), AP scanning is rejected for 5 seconds, thereby not missing the client association request. <p>disabled</p>
beacon-period	<p>Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.</p> <p>60 (minimum) 100 milliseconds</p>
beacon-regulate	<p>Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.</p> <p>disabled</p>
cap-reg-eirp <cap-reg-eirp>	<p>Work around a known issue on Cisco 7921G telephones by specifying a cap for a radio's maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.</p> <p>1–31 dBm</p>

Parameter	Description
<code>cell-size-reduction <cell-size-reduction></code>	<p>The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issues. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.</p> <p>Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.</p> <p>1-55dB 0 dB</p>
<code>channel</code>	<p>Channel number for the AP 802.11g/802.11n.802.11ac physical layer. The available channels depend on the regulatory domain (country). This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface.</p> <p>Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes:</p> <ul style="list-style-type: none"> ▪ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ▪ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ▪ num-: Entering a channel number with a minus (-) sign selects a primary and

Parameter	Description
	<p>secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel.</p> <p>NOTE: 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.</p> <p>Depends on regulatory domain</p>
clone	Name of an existing radio profile from which parameter values are copied.
csa	<p>Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.</p> <p>disabled</p>
csa-count	<p>Number of CSA announcements that are sent before the AP begins transmitting on the new channel.</p> <p>1-16</p> <p>4</p>
channel-reuse	<p>When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.)</p> <ul style="list-style-type: none"> ▪ Static mode: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ▪ Dynamic mode: In this mode, the Clear

Parameter	Description
	<p>Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client.</p> <ul style="list-style-type: none"> ▪ Disable mode: This mode does not support the tuning of the CCA Detect Threshold. <p>enabled, disabled enabled</p>
channel-reuse-threshold	<p>RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm.</p> <p>If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold.</p> <p>Depends on regulatory domain</p>
deploy-hour <0-23>	<p>Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. If this parameter is set in both the AirMatch profile and the 802.11g radio profile, the setting in the 802.11g radio profile will take precedence.</p> <p>0-23 5</p>

Parameter	Description
disable-arm-wids-functions	<p>Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option.</p> <p>CAUTION: Use carefully, since this effectively disables ARM and WIDS.</p> <p>disabled</p>
dot11b-protection	<p>Enable or disable protection for 802.11b clients. This parameter is enabled by default. Disabling this feature may improve performance if there are no 802.11b clients on the WLAN.</p> <p>WARNING: Disabling protection violates the 802.11 standard and may cause interoperability issues. If this feature is disabled on a WLAN with 802.11b clients, the 802.11b clients will not detect an 802.11g client talking and can potentially transmit at the same time, thus garbling both frames.</p> <p>enabled</p>
dot11h	<p>Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities</p> <p>disabled</p>
eirp-max	<p>Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33 or 127 9</p>
eirp-min	<p>The minimum transmission power level (in dBm) to be assigned to the AP radio(s).</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p>

Parameter	Description
	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33 or 127 6
eirp-offset	<p>Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.</p> <p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>-6 to 6 dBm 0 dBm</p>
energy-detect-threshold	<p>Modify the Energy Detect Threshold (EDT) used by the radio in making transmit decisions. The EDT is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm.</p> <p>Specify a value of 0 to use the default EDT for this radio. (This value may vary by AP model)</p> <p>0, 1-12 0 (disabled)</p>
frame-bursting-mode	<p>In some dense deployments, it is possible for APs to hear other APs on the same channel. This creates co-channel interference where the traffic of an active client could affect the air traffic of neighboring APs within the same channel. Starting from ArubaOS 8.11.0.0, users are allowed to control frame bursting even if there's only one active client associated to the AP.</p> <ul style="list-style-type: none"> ■ Dynamic: Frame bursting will be enabled only when one active client is connected to the AP, and frame bursting will be disabled when there is more than one active client. ■ OFF: Frame bursting mode is always disabled. ■ ON: Frame bursting mode is always enabled.
high-efficiency-enable <radio>	<p>Enables high-efficiency (802.11ax) features on a radio using the 2.4 GHz frequency band.</p> <p>enabled</p>

Parameter	Description
high-throughput-enable	Enables high-throughput (802.11n) features on a radio using the 2.4 GHz frequency band. enabled
ht-radio-profile	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See rf ht-radio-profile on page 1249 . default-a
interference-immunity	Set a value for 802.11 interference immunity. This parameter sets the interference immunity on the 2.4 GHz band. When performance drops due to interference from non- 802.11 interferers (such as DECT or Bluetooth devices), the level can be increased for improved performance. There are 17 levels (0-16) and Table 10 lists the settings applied for each level. NOTE: It is recommended not to adjust interference immunity without guidance from Aruba support. Increasing the immunity level in a healthy network may result in severe loss of performance. This should be set to a higher than default level only when there is significant degradation due to non-Wi-Fi interference. 0-16 2
iot-coex-enable	Enables WLAN co-existence feature with IoT and avoids simultaneous transmissions. enabled
max-channel-bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Conductor managed devices. NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller. 20MHz, 40MHz, 80MHz or 160MHz 80MHz
min-channel-bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Conductor managed devices.

Parameter	Description
	<p>NOTE: This parameter is only supported on Mobility Conductor, and is not available in on a standalone controller.</p> <p>20MHz, 40MHz, 80MHz 20MHz</p>
maximum-distance	<p>Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 2.4GHz frequency band radio:</p> <ul style="list-style-type: none"> ▪ 20MHz mode: 54km ▪ 40MHz mode: 24km <p>Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.</p> <p>0-24km (40MHz mode), 0-54km (20MHz mode) 0 meters</p>
mgmt-frame-throttle-interval	<p>Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-60 1 second interval</p>
mgmt-frame-throttle-limit	<p>Maximum number of management frames allowed in each throttle interval.</p> <p>NOTE: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.</p> <p>0-999999 20 frames per interval</p>
mode	<p>One of the operating modes for the AP. ap-mode</p>

Parameter	Description
ap-mode	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.
am-mode	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
spectrum-mode	Device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.
no	Negates any configured parameter.
rts-mode	RTS mode allows users to control RTS frame transmission to the clients. <ul style="list-style-type: none"> ■ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ■ always-disable: RTS is not used for any transmission. ■ default: The default RTS mode configured in the wireless driver of the AP is used. For 300 Series, 310 Series, 360 Series, 370 Series, AP-387, 530 Series, AP-555, 580 Series, 630 Series, and 635 Series access points, RTS is used for every alternate retried PPDU transmission. For 500H Series, 500 Series, 510 Series, 560 Series, 570 Series, 610 Series access points, RTS is used for all AMPDU transmissions. default
radio-enable	Enables or disables radio configuration. enabled
slb-mode channel radio	SLB Mode allows control over how to balance clients. Select one of the following options: <ul style="list-style-type: none"> ■ channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ radio: Radio-based load-balancing balances clients across APs channel

Parameter	Description
s1b-threshold	<p>If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.</p> <p>1-100%</p> <p>20%</p>
s1b-update-interval <secs>	<p>Specify how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.</p> <p>1-2147483647 seconds</p> <p>30 seconds</p>
smart-antenna	<p>Enable or disable the smart antenna feature on AP-335 access points.</p> <p>enabled, disabled</p> <p>enabled</p>
spectrum-load-bal-domain	<p>Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment.</p> <ul style="list-style-type: none"> ■ If spectrum load balancing is enabled in a 802.11g radio profile but the spectrum load balancing domain is <i>not</i> defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11g radio profile and a spectrum load balancing domain <i>isalso</i> defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.

Parameter	Description
spectrum-load-balancing	<p>The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP.</p> <p>disabled</p>
spectrum-monitoring	<p>Issue this command to turn APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.</p> <p>For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.x User Guide.</p> <p>default</p>
spectrum-profile <profile>	<p>Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 1254.</p> <p>default</p>
transmit	<p>Enable or disable transmission of frames on the radio.</p> <p>NOTE: This parameter should only be used for radio test purposes.</p> <p>enabled, disabled</p> <p>disabled</p>
tx-power	<p>Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration.</p>

Parameter	Description
	<p>This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities.</p> <p>NOTE: This parameter is only supported on a standalone controller, and is not available in the Mobility Conductor command-line interface.</p> <p>-51 dBm to 51 dBm 14 dBm</p>
very-high-throughput-rates-enable	<p>This feature enables Very High Throughput (VHT) rates on the 2.4 GHz band, providing 256-QAM modulation and encoding that allows for 600 Mbit/sec performance over 802.11n networks. Maximum data rates are increased on the 2.4 GHz band through the addition of VHT Modulation and Coding Scheme (MCS) values 8 and 9, which support the highly efficient modulation rates in 256-QAM. Starting with ArubaOS 6.4.2.0, VHT is supported on 220 Series access points on both 20 and 40 MHz channels.</p> <p>Using the controller's CLI or WebUI, VHT MCS values 0-9 are enabled, overriding the existing high-throughput (HT) MCS values 0-7, which have a lower maximum data rate. However, this feature should be disabled if individual rate selection is required.</p> <p>disabled</p>

The following table indicates values for a range of distances:

Timeouts[usec] Distance[m]	5GHz radio			2.4GHz radio		
	Ack	CTS	Slot	Ack	CTS	Slot
0 (outdoor:16050m)	128	128	63	128	128	63
0 (indoor:600a,6450g)	25	25	9	64	48	9
200 (==default)	25	25	9	64	48	9
500	25	25	9	64	48	9
600	25	25	9	64	48	9
1050	28	28	13	64	48	31
5100	55	55	26	64	55	31
10050	88	88	43	88	88	43
15000	121	121	59	121	121	59
16050	128	128	63	128	128	63
58200 (5G limit 20M)	409	409	203	-	-	-

```

52650 (2.4G limit 20M) - - - 372 372 185
27450 (5G limit 40M) 204 204 101 - - -
24750 (2.4G limit 40M) - - - 186 186 92

```

Examples

The following command configures APs to operate in AM mode for the selected dot11g-radio-profile named "sample-g".

```

(host)[mynode](config)#rf dot11g-radio-profile sample-g
mode am-mode

```

The following command configures APs to operate in high-throughput (802.11n) mode on the 2.4 GHz frequency band for the selected dot11g-radio profile named "sample-g" and assigns a high-throughput radio profile named "default-g".

```

(host)[mynode](config)#rf dot11g-radio-profile sample-g
high-throughput-enable
ht-radio-profile default-g

```

The following command configures a primary channel number of 1 and a secondary channel number of 5 for 40 MHz mode of operation with the dot11g-radio profile named "sample-g".

```

(host)[mynode](config)# rf dot11g-radio-profile sample-g channel <1+>

```

The following table indicates the interference immunity implementation for each level.

Table 10: *Interference Immunity Levels*

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
0	Disabled	Disabled	Enabled	None	None
1	Enabled	Disabled	Enabled	None	None
2	Enabled	Enabled	Enabled	None	None
3	Enabled	Enabled	Enabled	None	None

Immunity Level	Adaptive Noise Immunity (ANI)	Preemption Mode	Low Noise Amplifier (LNA)	Interference Sensitivity Reduction	Force Noise Floor (for 2.4 GHz radio only)
4	Enabled	Enabled	Enabled	4 dB	None
5	Enabled	Enabled	Enabled	8 dB	None
6	Enabled	Enabled	Enabled	12 dB	None
7	Enabled	Enabled	Enabled	16 dB	None
8	Enabled	Enabled	Enabled	None	-85 dB
9	Enabled	Enabled	Enabled	None	-80 dB
10	Enabled	Enabled	Enabled	None	-75 dB
11	Enabled	Enabled	Enabled	8 dB	-85 dB
12	Enabled	Enabled	Enabled	8 dB	-80 dB
13	Enabled	Enabled	Enabled	None	None
14	Enabled	Enabled	Enabled	None	None
15	Enabled	Enabled	Enabled	8 dB	None
16	Enabled	Enabled	Enabled	16 dB	None

- **Adaptive Noise Immunity:** Adjust noise and spur immunity levels based on PHY errors.
- **Preemption mode:** The radio stops current reception and restarts the receiver when a new signal which is above the threshold of the current signal is found. This allows the radio to switch signals when it locks onto interference or weaker 802.11 signal, when a valid 802.11 signal with a higher signal strength is detected.
- **Low Noise Amplifier:** Enables radio saturation at lower signal levels resulting in better performance in the presence of interference. Disabling LNA avoids radio saturation at lower signal levels. However, it may reduce range and throughput.
- **Interference Sensitivity Reduction:** Reduces the sensitivity to both Wi-Fi and non Wi-Fi interference signals. This makes the radio deaf to signals in which the SNR is below the threshold.
- **Force Noise Floor (for 2.4 GHz radio only):** Forces the radio to use the configured value as the absolute noise floor value. This makes the radio ignore signals of weaker amplitude.

Command History

Release	Modification
ArubaOS 8.11.0.0	The frame-bursting-mode and rts-mode parameters were introduced.
ArubaOS 8.10.0.0	The <code>airmatch-mode-aware</code> parameter was added.
ArubaOS 8.8.0.0	The <code>iot-coex-enable</code> parameter was added.
ArubaOS 8.4.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>high-efficiency-enable <radio></code> ■ <code>assoc-boost</code>
ArubaOS 8.1.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ <code>deploy-hour</code> ■ <code>eirp-offset</code> ■ <code>energy-detect-threshold</code> ■ <code>minimum-channel-bandwidth</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf event-thresholds-profile

```
rf event-thresholds-profile <profile>
  bwr-high-wm <percent>
  bwr-low-wm <percent>
  clone <profile>
  detect-frame-rate-anomalies
  fer-high-wm <percent>
  fer-low-wm <percent>
  ffr-high-wm <percent>
  ffr-low-wm <percent>
  flsr-high-wm <percent>
  flsr-low-wm <percent>
  fnur-high-wm <percent>
  fnur-low-wm <percent>
  frer-high-wm <percent>
  frer-low-wm <percent>
  frr-high-wm <percent>
  frr-low-wm <percent>
  no ...
```

Description

This command configures the event thresholds profile. The event threshold profile configures Received Signal Strength Indication (RSSI) metrics. When certain RF parameters are exceeded, these events can signal excessive load on the network, excessive interference, or faulty equipment. This profile and many of the detection parameters are disabled (value is 0) by default.

Parameter	Description
<profile>	Name of this instance of the profile. The name must be 1-63 characters. default
bwr-high-wm	If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%. 0-100 0%
bwr-low-wm	After a bandwidth exceeded condition exists, the condition persists until bandwidth drops below this value. The recommended value is 70%. 0-100 0%

Parameter	Description
clone	Name of an existing radio profile from which parameter values are copied.
detect-frame-rate-anomalies	Enable or disables detection of frame rate anomalies. disabled
fer-high-wm	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%. 0-100 0%
fer-low-wm	After a frame error rate exceeded condition exists, the condition persists until the frame error rate drops below this value. The recommended value is 8%. 0-100 0%
ffr-high-wm	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%. 0-100 16%
ffr-low-wm	After a frame fragmentation rate exceeded condition exists, the condition persists until the frame fragmentation rate drops below this value. The recommended value is 8%. 0-100 8%
flsr-high-wm	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%. 0-100 16%
flsr-low-wm	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value. The recommended value is 8%. 0-100 8%

Parameter	Description
fnur-high-wm	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, a non-unicast rate exceeded condition exists. This value depends upon the applications used on the network. 0-100 0%
fnur-low-wm	After a non-unicast rate exceeded condition exists, the condition persists until the non-unicast rate drops below this value. 0-100 0%
frer-high-wm	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, a frame receive error rate exceeded condition exists. The recommended value is 16%. 0-100 16%
frer-low-wm	After a frame receive error rate exceeded condition exists, the condition persists until the frame receive error rate drops below this value. The recommended value is 8%. 0-100 8%
frr-high-wm	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, a frame retry rate exceeded condition exists. The recommended value is 16%. 0-100 16%
frr-low-wm	After a frame retry rate exceeded condition exists, the condition persists until the frame retry rate drops below this value. The recommended value is 8%. 0-100 8%
no	Negates any configured parameter.

Example

The following command configures an event threshold profile:

```
(host)[node](config) #rf event-thresholds-profile et1
```

```
detect-frame-rate-anomalies
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf ht-radio-profile

```
rf ht-radio-profile <profile>
  40MHz-intolerance
  bss-color <bss-color>
  bss-color-switch-count
  clone <profile>
  csd-override
  honor-40MHz-intolerance
  no
  vht-bw-signaling
  vht-txbf-sounding-interval
```

Description

This command configures high-throughput AP radio settings. High-throughput features use the IEEE 802.11n standard, which supports 40 MHz channels and operates in both the 2.4 GHz and 5 GHz frequency bands.

Most transmissions to high throughput (HT) stations are sent through multiple antennas using cyclic shift diversity (CSD). When you enable the disable-diversity-spreading parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). Note, however, that enabling this feature can reduce overall throughput rates.

The ht-radio-profile you wish to use must be assigned to a dot11a and/or dot11g-radio-profile. You can assign the same profile or different profiles to the 2.4 GHz and 5 GHz frequency bands. See [rf dot11a-radio-profile on page 1196](#) and [rf dot11g-radio-profile on page 1228](#).

Parameter	Description
<profile>	Name of this instance of the profile. The name must be 1-63 characters. Default Options: <ul style="list-style-type: none">■ "Default-a" is generally used in association with high-throughput devices running on the 5 GHz frequency band, see rf dot11a-radio-profile on page 1196.■ "Default-g" is generally used in association with high-throughput devices running on the 2.4 GHz frequency band, see rf dot11g-radio-profile on page 1228.■ "Default" is generally used when the same ht-radio-profile is desired for use with both frequency bands. default-a, default-g, default
40MHz-intolerance	Controls whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed. disabled

Parameter	Description
<code>bss-color</code>	<p>Enables different colors for each category of BSSIDs. The Aruba 802.11ax based access points like AP-505, AP-515, AP-534, AP-535 and AP-555 support BSS coloring mechanism that helps identify the BSS from which a PLCP protocol data unit originates.</p> <p>NOTE: 530 Series and 550 Series access points can detect and change the color automatically if the same color is detected for another BSS on the same channel.</p> <p>NOTE: The value of 0 means auto mode, that is, the AP will set the color by itself, finding any available color.</p> <p>0-63 0</p>
<code>bss-color-switch-count</code>	<p>The number of times the BSS color switch announcements are sent in beacons before switching to a new color. Range: 0-100 and the default value is 10.</p> <p>0-100 10</p>
<code>clone</code>	<p>Name of an existing high-throughput radio profile from which parameter values are copied.</p>
<code>csd-override</code>	<p>Override Cyclic Shift Diversity for better interoperability.</p>
<code>honor-40MHz-intolerance</code>	<p>When enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.</p> <p>enabled</p>
<code>no</code>	<p>Negates any configured parameter.</p>
<code>vht-bw-signaling</code>	<p>Enable VHT Bandwidth Signaling RTS for better interoperability (802.11ac APs only).</p> <p>Disabled</p>
<code>vht-txbf-sounding-interval</code> < <code>vht-txbf-sounding-interval</code> >	<p>Time interval in milliseconds between updates of VHT Transmit Beamforming channel estimation. (802.11ac APs only).</p> <p>0</p>

Example

The following command configures an ht-radio-profile named "default-g" and enables 40MHz-intolerance:

```
(host) [node] (config) #rf ht-radio-profile default-g  
40MHz-intolerance
```

Command History

Release	Modification
ArubaOS 8.6.0.0	The <code>bss-color-switch-count</code> parameter was added.
ArubaOS 8.4.0.0	The <code>bss-color</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, but operates with IEEE 802.11n compliant devices only	Base operating system.	Config mode on Mobility Conductor.

rf optimization-profile

```
rf optimization-profile <profile-name>
  clone <profile>
  handoff-assist
  low-rssi-threshold <number>
  no ...
  rssi-check-frequency <number>
  rssi-falloff-wait-time <number>
```

Description

This command configures the RF optimization profile.

Parameter	Description
<profile-name>	Name of this instance of the profile. The name must be 1-63 characters. default
clone	Name of an existing optimization profile from which parameter values are copied.
handoff-assist	Allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold. disabled
low-rssi-threshold	Minimum RSSI, above which deauth should never be sent. 1-255 10
no	Negates any configured parameter.
rssi-check-frequency	Interval, in seconds, to sample RSSI. 9-255 seconds 3 seconds
rssi-falloff-wait-time <number>	Number of times the detected client RSSI level must fall below the minimum RSSI threshold the before the AP sends a deauthorization message to the client. The maximum value is 8 times. 0-8 4

Example

The following command configures an RF optimization profile:


```
(host)[node](config) #rf optimization-profile Angela1
(host)[node](RF Optimization Profile "Angela1") #rssi-falloff-wait-time 3
(host)[node](RF Optimization Profile "Angela1") #rssi-check-frequency 2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

rf spectrum-profile

```
rf spectrum-profile <profile-name>
  age-out audio|bluetooth|cordless-ff-phone|cordless-fh-base|cordless-fh-
  network|generic-ff|generic-fh|microwave|microwave-
  inverter|unknown|video|wifi|xbox
  channel
  clone <source>
  fft-dwell-time-ap
  fft-format
  fft_capture_ip
  filter-channel
  no ...
  no-wifi-fft
```

Description

Define the device ageout times used by a spectrum monitor, or hybrid AP radio. The Spectrum Analysis software module provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify the 802.11 devices on the network. APs that gather spectrum data are called Spectrum Monitors, or *SMs*, and reference a spectrum profile that determines the band monitored by that SM radio. Use this profile to modify default device ageout times for spectrum monitors and hybrid APs using this profile.

For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS User Guide.

Parameter	Description
age-out	Use the age-out parameter to define the number of seconds for which a specific device type must stop sending a signal before the spectrum monitor considers that device no longer active on the network.
audio	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as Fixed Frequency (Audio). 5-65535 seconds 10 seconds
bluetooth	Bluetooth devices. Note that this setting is applicable to 2.4GHz spectrum monitor radios only. 5-65535 seconds 25 seconds

Parameter	Description
cordless-ff-phone	<p>Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as Fixed Frequency (Cordless Phones).</p> <p>5-65535 seconds</p> <p>10 seconds</p>
cordless-fh-base	<p>Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as Frequency Hopper (Cordless Base).</p> <p>5-65535 seconds</p> <p>240 seconds</p>
cordless-fh-network	<p>When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as Frequency Hopper (Cordless Network). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.</p> <p>5-65535 seconds</p> <p>60 seconds</p>
generic-ff	<p>All fixed frequency devices that do not fall into one of the other categories are classified as Fixed Frequency (Other). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).</p> <p>5-65535 seconds</p> <p>10 seconds</p>
generic-fh	<p>When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.</p> <p>5-65535 seconds</p> <p>25 seconds</p>

Parameter	Description
generic-interferer	<p>Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a Generic Interferer. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.</p> <p>5-65535 seconds 30 seconds</p>
lteu	<p>LTE-U Fixed Frequency devices</p> <p>5-65535 seconds 10 seconds</p>
microwave	<p>Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.</p> <p>5-65535 seconds 15 seconds</p>
microwave-inverter	<p>Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as Microwave (Inverter). Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).</p> <p>5-65535 seconds 15 seconds</p>
video	<p>Video transmitters that continuously transmit video on a single frequency are classified as Fixed Frequency (Video). These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.</p> <p>5-65535 seconds 60 seconds</p>

Parameter	Description
wifi	Wi-Fi devices. 5-65535 seconds 600 seconds
xbox	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as Frequency Hopper (Xbox). Note that this setting is applicable to 2.4GHz spectrum monitor radios only. 5-65535 seconds 25 seconds
channel <channel>	Scan this channel for spectrum FFT.
clone <source>	Make a copy of an existing spectrum profile. 600 seconds
fft-dwell-time-ap	Specify the number of msec FFTs that will be enabled in hybrid mode (802.11ac APs only). Range: 5 - 900 msec. . 5-900 milliseconds 20 millisecond
fft-format	Specify one of the following power format of frequency bins for FFTs on QCA APs with V2 FFT format: <ul style="list-style-type: none"> 0: linear magnitude 1: log magnitude
fft_capture_ip <fft_capture_ip>	Specify the IP address where the AP sends the captured FFT samples.
filter-channel <filter-channel>	Specify the channel for which the data is to be passed to the classifier.
no	Remove a spectrum profile or negate a configured parameter.
no-wifi-fft	Specify weather the WiFi packets should be displayed in FFT charts. <ul style="list-style-type: none"> 0 : Display WiFi. 1 : Do not display WiFi.

Example

The following command creates the spectrum profile **spectrum2**.



```
(host)[node](config) #rf spectrum-profile spectrum2
```

Related Commands

Command	Description
show ap mesh-ht-ssid-profile	Shows a spectrum profile used by the spectrum analysis feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license.	Config mode on Mobility Conductor.

router mobile

router mobile

Description

This command enables Layer-3 (IP) mobility on a controller. IP mobility is disabled by default on the controller. This command must be executed on all controllers(master/ conductor and local) that need to provide support for layer-3 roaming in a mobility domain. You can enable or disable IP mobility on a virtual AP profile with the `wlan virtual-ap` command (IP mobility is enabled by default in a virtual AP profile).



It is recommended to reboot the controller every time you enable or disable IP mobility.

Example

This command enables IP mobility:

```
(host) [mynode] (config) #router mobile
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

router ospf

```
router ospf
  aggregate-route rapng-vpn <addr> <mask>
  area <area-id>
    default-cost <cost>
    no [default-cost | nssa | stub]
    nssa [default-information-originate | no-redistribution | no-summary]
    stub [no-summary]
  default-information originate always
  redistribute
    ike-overlay
    loopback
    rapng-vpn
    static
    vlan [add <vlan-ids> | remove <vlan-ids> | <vlan-ids>]
  router-id <rtr-id>
  subnet exclude <addr> <mask>
```

Description

This command configures OSPF configuration for the upstream router. This command is only available in the Config mode. OSPFv2 is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The OSPF implementation allows managed devices to deploy effectively in a Layer 3 topology.

Parameter	Description
aggregate-route rapng-vpn <addr> <mask>	Configures the aggregate route information for specified IP address and subnet mask and redistributes RAPNG VPN address.
area <area-id>	Configures OSPF area for specified area ID (IP address).
default-cost <cost>	Configures summary default-cost of a NSSA/stub area. 0-16777215
no [default-cost nssa stub]	Removes configured default-cost of NSSA/stub, NSSA, or stub.
nssa [default-information-originate no-redistribution no-summary]	Configures origination of type 7 default into NSSA area, sets NSSA area for no distribution into this NSSA area, or stops sending of summary LSA into this NSSA area.
stub [no-summary]	Configures an area as stub area and stops sending summary LSA into this area.

Parameter	Description
<code>default-information originate always</code>	Configures distribution of default information by distributing a default route.
<code>redistribute</code>	Redistributes the route.
<code>ike-overlay</code>	Redistributes Ike overlay routes.
<code>loopback</code>	Redistributes loopback addresses.
<code>rapng-vpn</code>	Redistributes RAPNG VPN addresses.
<code>static</code>	Redistributes static IP routes.
<code>vlan [add <vlan-ids> remove <vlan-ids> <vlan-ids>]</code>	Redistributes VLAN user subnet, adds user VLANs to list, or removes user VLANs from list.
<code>router-id <rtr-id></code>	Configures router ID for specified IP address
<code>subnet exclude <addr> <mask></code>	Configures IP address and subnet mask that OSPF will not advertise

Example

The following example configures an IP address 192.0.2.1 and subnet mask 255.0.255.255 that OSPF will not advertise:

```
(host) [mynode] (config) #router ospf subnet exclude 192.0.2.1 255.0.255.255
```

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>static</code> sub-parameter was added under the <code>redistribute</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Configuration mode on managed devices.

routing-policy-map

```
routing-policy-map
  branch <XX:XX:XX:XX:XX:XX> access-list <STRING>
  role <STRING> access-list <STRING>
```

Description

This command associates a routing ACL with a specific user role on a managed device. The commands to associate an access list to a user role vary, depending upon the type of access list being associated to that role. Ethertype, MAC, and session ACLs are applied globally across all managed devices, but routing access lists may vary between locations, so they are mapped to a user role in a local configuration setting.

In an environment where an IPsec map defines the connections between the managed device and Mobility Conductor, the global ACL **master/ conductor -boc-traffic** is applied to all IPsec maps between the managed device and Mobility Conductor. If any managed device requires a different ACL, issue the command `routing-policy-map branch <mac-addr> access-list <acl>` on that managed device to associate a different ACL to the L3 GRE tunnel between that one managed device and Mobility Conductor. This local setting will override the global settings defined in the **master/ conductor -boc-traffic** ACL.

Parameter	Description
branch <XX:XX:XX:XX:XX:XX>	By default, when a branch office deployment uses IPsec maps to define the connections between each branch office managed device and its Mobility Conductor, the global ACL master-boc-traffic is applied to those IPsec maps. Use this command to apply a local ACL to the GRE tunnel between a specific branch office managed device and its Mobility Conductor, overriding the default master/ conductor -boc-traffic ACL.
role <STRING>	Name of the user role to be associated with the specified routing ACL.
access-list <STRING>	Name of the route ACL to be associated to the specified user role.

Example

The following example maps a user role to a routing ACL.

```
(host)[node](config) #routing-policy-map
role employee access-list branch1
```



To associate the user role with an ethertype, MAC or session ACL, use the command `user-role <role> access-list eth|mac|session <acl>`.

Related Commands

Command	Description
ip access-list route	Configures an ACL for policy-based routing (PBR).
ip nexthop-list	Defines a next-hop list for a routing policy.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

sc-migration

```
sc-migration
  dbupdate
  downgrade <ip>
  export sc-ca-cert {self-signed-cert|<custom-cert>}
  import <ip>
```

Description

This command is used by the migration tool to export and import migration data from controllers in ArubaOS 6.x deployments to ArubaOS 8.x deployment.

Parameter	Description
dbupdate	Update the database entries for standalone system.
downgrade	Downgrade the databases.
<ip>	IP Address for GAP or WMS database that has to be downgraded.
export	Exports the setup data into <i>/tmp/dbsync/migration/setupInfo.xml</i>
sc-ca-cert [self-signed-cert <custom-cert>]	(Optional) Specify the CA certificate to be sent to the managed device. You can specify one of the following certificates: <ul style="list-style-type: none">■ self-signed-cert—Self-signed CA certificate is exported into <i>/tmp/dbsync/migration/sc_ssc.pem</i>■ <custom-cert>—The specified custom certificate (<i>/flash/certmgr/TrustedCA/<custom-cert></i>) is exported into <i>/tmp/dbsync/migration/<custom-cert></i>
import <ip>	Runs the upgrade scripts on the configuration (<i>default.cfg</i>) stored in the specified IP address. The upgraded configuration is applied on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on managed device.

scheduler-profile

```
scheduler-profile <profile>
  clone
  priority-map q0|q1|q2|q3 <que-prio-list>
  queue-weights q0|q1|q2|q3 <que-weight>
```

Description

Define a scheduler profile that associates priorities to four uplink queues.

Parameter	Description
<code>clone <profile></code>	Make a copy of an existing scheduler profile.
<code>priority map q0 q1 q2 q3 <que-prio-list></code>	Specify one or more priority levels (0-7) for each queue type (q0 through q3). Each of the seven priority levels must be supported by one of the four queues.
<code>queue-weights q0 q1 q2 q3 <que-weight></code>	(Optional) Enter the percentage of available bandwidth that should be made available to traffic in each of the four queues. If you do not specify a weight for each queue, the queue service is based exclusively on the priority of the queue, where the lower priority queues are not serviced until the higher priority queue is clear. With this option, the highest level priority is guaranteed as much bandwidth as possible, but there can be phases where the 2nd, 3rd and 4th priority queues may receive little or no bandwidth.

Example

ArubaOS supports minimum bandwidth guarantees per traffic class, and allows critical delay-sensitive applications like voice and video to use more bandwidth and/or be scheduled with higher priority. Each interface can be associated with a scheduler profile, that supports four queues with different priority levels. If you use session ACLs to define traffic policies on the managed device, you can use the scheduler profile to automatically associate these different priority levels assigned by these policies to a scheduler profile queue. The scheduler profile must be associated with an interface using the command `interface cellular|gigabitethernet <slot/module/port> transmit max-rate rate mbits <mbps> scheduler-profile <profile>`.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

scm

```
scm disable dds-replication
```

Description

This command is used to disable DDS replication.

Example

```
(host)[mynode] (config) #scm disable dds-replication
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

scs-local-custom-cert

```
scs-local-custom-cert [scs-local-mac <mac>] [ca-cert <ca>] [server-cert <sc>]  
[suite-b [gcm128] | [gcm256]]
```

Description

This command configures security for all master/ conductor -local control traffic using custom certificate.

Parameter	Description
scs-local-mac <mac>	Specifies MAC address of managed device.
ca-cert <ca>	Specifies CA certificate to use.
server-cert <sc>	Specifies server certificate to use.
suite-b	Specifies GCM-128 or GCM-256 suite B algorithm to use.

Example

The following example configures CA certificate **default_ca** and server certificate **default_server** for master/ conductor -local control traffic:

```
(host) [mynode] #scs-local-custom-cert scs-local-mac  
00:1a:1e:aa:bb:cc ca-cert default_ca server-cert default_server
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

sdwan-profile

```
sdwan-profile
  enable
  no enable
```

Description

This command is used to enable or disable an SD-WAN profile.

Parameter	Description
enable	This parameter is used to enable an SD-WAN profile. Default: Disabled
no enable	This parameter is used to delete an SD-WAN profile.

Example

```
(host) [mynode] (config) #sdwan-profile
(host) [mynode] (sdwan-profile) #no enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base Operating System	Config mode on Mobility Conductor.

secondary masterip/secondary conductorip

```
secondary masterip/secondary conductorip <secmasterip_val>/<seconductorip_val>  
[ipsec | ipsec-custom-cert | ipsec-factory-cert | vpn-ip]
```

Description

Use this command to add a secondary Mobility Conductor from the primary Mobility Conductor CLI. This command is allowed in the **/md** tree, both in device nodes and group nodes.

Parameter	Description
secmasterip_val/seconductorip_val	Configure the master IP address or FQDN.
ipsec <key>	IPSec key of length 64 bytes.
fqdn <local-fqdn>	The Local's FQDN (max 64 bytes) used in IKE. This is optional for a Dynamically addressed Local
interface vlan <id>	Vlan interface to initiate IKE. The switch IP will be used if the vlan is not specified.
peer-mac-1 <peermac-1>	Specify peer MAC string.
ipsec-custom-cert	Custom Cert-based IPSec secure communication between master/ conductor and local.
master-mac-1-c <mac-1-c>/ conductor-mac-1-c <mac-1-c>	Specify Master's/Conductor's MAC address.
ca-cert	Specify the CA certificate to use.
master-mac-2-c	Specify the redundant master's MAC address.
ipsec-factory-cert	Factory Cert-based IPSec secure communication between master / conductor and local.
master-mac-1/conductor-mac-1	Specify Master's/Conductor's MAC address.
vpn-ip <vpnip>	VPN concentrator's IP address or FQDN.

Example

The following command enables you to add a secondary Mobility Conductor.

```
(host) [md] (config) #secondary masterip
```

Related Commands

Command	Description
master-l3redundancy/conductor-l3redundancy	Configures Layer-3 redundancy for a Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

secondary masteripv6/secondary conductoripv6

```
secondary masteripv6/secondary conductoripv6 <secmasteripv6_val>/<seconductoripv6_val> [ipsec <KEY> {fqdn <local-fqdn>|interface <vlan> {<id>}}|masteripv4 <secmasteripv4_val>/<seconductoripv4_val>|peer-mac-1 <peermac-1> ipsec-custom-cert [master-mac-1-c <MAC>] ipsec-factory-cert [master-mac-1-c <MAC>] vpn-ipv6
```

Description

Use this command to add a secondary Mobility Conductor containing IPv6 address. This command allows the user to add a secondary Mobility Conductor from the primary Mobility Conductor CLI. This command is allowed in the **/md** tree, both in device nodes and group nodes.

Parameter	Description
secmasteripv6_val/<seconductoripv6_val>	Configure the secondary master ipv6 address or FQDN.
ipsec <KEY>	Configure the IPsec secure communication between master/ conductor and local controllers. The IPsec key is of length 64 bytes.
fqdn <local-fqdn>	Configure the local controller's FQDN (max 64 bytes) used in IKE. This is optional for a dynamically addressed device.
interface <vlan> {<id>}	Configure the VLAN interface to initiate IKE. The switch IP is used if the vlan is not specified.
masteripv4/conductoripv4 <secmasteripv4_val>/<seconductoripv4_val>	Configure the corresponding IPv4 address of secondary master/ conductor . The configuration of the masteripv4 <secmasteripv4_val> sub-parameter is optional in a native IPv6 deployment.
peer-mac-1 <peermac-1>	Specify the peer MAC string on the primary Mobility Conductor.

Parameter	Description
<code>ipsec-custom-cert</code>	Custom certificate-based IPsec secure communication between master/ conductor and local controllers.
<code>master-mac-1-c <MAC>/conductor-mac-1-c<mac-1-c></code>	Specify the MAC address on the Mobility Conductor.
<code>ca-cert</code>	Specify the CA certificate to use.
<code>master-mac-2-c</code>	Specify the redundant master's MAC address.
<code>ipsec-factory-cert</code>	Factory certificate-based IPsec secure communication between master/ conductor and local controllers.
<code>master-mac-1-c <MAC>/conductor-mac-1-c <MAC></code>	Specify the MAC address on the Mobility Conductor.
<code>vpn-ipv6</code>	VPN concentrator's IPv6 address or FQDN.

Example

The following command enables you to add a secondary Mobility Conductor.

```
(host) [mynode] (config) #secondary masteripv6/secondary conductoripv6
```

The following example configures the managed device with an IPsec pre-shared key on the secondary Mobility Conductor:

```
(host) *[mynode] (config) #secondary masteripv6/secondary conductoripv6
2021:1:1:145::109 ipsec itsabug peer-mac-1 00:0C:29:60:92:E2 peer-mac-2
00:15:5D:14:1F:06 interface vlan 47 masteripv4 10.16.145.109
```

The following example configures the managed device with a factory-installed certificate on the secondary Mobility Conductor:

```
(host) *[mynode] (config) #secondary masteripv6/secondary conductoripv6
2001:78::245 ipsec-factory-cert master-mac-1 20:4c:03:0e:e1:68 interface-f
vlan-f 79 masteripv4 10.15.78.245
```

The following command configures the managed device terminating through VPNC with a factory-installed certificate on the secondary Mobility Conductor:

```
(host) *[mynode] (config) #secondary masteripv6/secondary conductoripv6
2021:1:1:145::109 vpn-ipv6 2001:192:192::8 ipsec-factory-cert vpn-mac-1
00:0b:86:b6:c7:07 interface vlan 172 masteripv4 10.16.145.109
```

The following command configures the managed device terminating through VPNC with a custom-installed certificate on the secondary Mobility Conductor:

```
(host) *[mynode] (config) #secondary masteripv6/secondary conductoripv6
2021:1:1:167::254 vpn-ipv6 2001:192:192::11 ipsec-custom-cert vpn-mac-1-c
00:0b:86:b6:c7:07 ca-cert-v BOC-CA server-cert-v BOC_cert interface vlan 172
masteripv4 10.16.167.254
```

Related Commands

Command	Description
master-l3redundancy/conductor-l3redundancy	Configures Layer-3 redundancy for a Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

serial console redirect

```
serial console redirect {enable | disable}
```

Description

This command configures redirect to serial console.

Parameter	Description
enable	Enables redirect to serial console.
disable	Disables redirect to serial console.

Example

Access the CLI and use the following command to enable the redirect to serial console:

```
(host) [mynode] #serial console redirect enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

service

```
service
  dhcp
  dhcpv6
  network-storage
  print-server
  scp
  no...
```

Description

This command enables the DHCP server on the controller. You can enable and configure DHCP, DHCPv6, network-storage, print server, or SCP in the controller to provide the following clients:

- **DHCP**: IP addresses to wireless clients if an external DHCP server is not available.
- **DHCPv6**: IPv6 addresses to wireless clients if an external DHCPv6 server is not available.
- **network-storage**: To provide access to the storage devices attached to the controller or managed device.
- **printer-server**: To provide access to printers attached to the controller .
- **SCP**: To provide SCP functionality on the controller itself rather than on an external server.

Parameter	Description
dhcp	Enables the DHCP server
dhcpv6	Enables the DHCPv6 server
network-storage	Enables the NAS service
print-server	Enables the printer service
scp	Enables the scp server functionality on the controller or managed device
no...	Removes the specific configuration

Example

The following command enables the DHCP server in the controller or managed device:

```
(host) [mynode] (config) #service dhcp
```

The following command enables the DHCPv6 server in the controller or managed device:

```
(host) [mynode] (config) #service dhcpv6
```

The following command enables the NAS services in the controller or managed device:

```
(host) [mynode] (config) #service network-storage
```

The following command enables the printer services in the controller or managed device:

```
(host) [mynode] (config) #service print-server
```

The following command enables the scp server functionality in the controller or managed device::

```
(host) [mynode] (config) #service scp
```

To disable the SCP server functionality on the controller, execute the following command:

```
(host) [mynode] (config) #no service scp
```

Related Commands

Command	Description
show scp	Shows if the SCP server functionality is enabled or not.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>scp</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on the controller or managed device.

session delete

session delete <ip>

Description

This command deletes a session.

Parameter	Description
<ip>	Deletes session of specified IP address.

Example

The following example deletes a session with IP address 192.0.2.1:

```
(host) [mynode] #session delete 192.0.2.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

set-ikepsk-by-addr

set-ikepsk-by-addr <ip-addr>

Description

This command configures IKE PSK corresponding to an IP address.

Parameter	Description
<ip-addr>	Configures specified IP address to use to select IKE PSK.

Example

Access the CLI and use the following command to configure IKE PSK corresponding to IP address **192.0.2.1**:

```
(host) [mynode] #set-ikepsk-by-addr 192.0.2.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

set-trust-anchor

```
set-trust-anchor {self-signed | <ca-name>}
```

Description

This command configures a trust anchor for an access point.

Parameter	Description
self-signed	Configures self signed certificate as the trust anchor.
<ca-name>	Configures the specified trusted CA certificate as the trust anchor.

Example

Access the CLI and use the following command to configure self-signed certificate for an access point:

```
(host) [mynode] #set-trust-anchor self-signed
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa auth-survivability

```
show aaa auth-survivability
```

Description

This command shows the authentication survivability configuration on a stand-alone controller.

Example

The following example shows the authentication survivability configuration:

```
(host) [mynode] #show aaa auth-survivability  
  
Auth-Survivability: Disabled (Not Running)  
Survival-Server Server-Cert: N/A  
Survival-Server Cache lifetime: 24 hours
```

Related Commands

Command	Description
aaa auth-survivability	This command configures Authentication Survivability on a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on stand-alone controller.

show aaa auth-survivability-cache

show aaa auth-survivability-cache

Description

This command shows the authentication survivability cached data on a stand-alone controller.

Example

The following example shows the authentication survivability cached data:

```
(host) [mynode] #show aaa auth-survivability-cache

Auth-Survivability Cached Data
-----
Station   User Name   Authenticated Using   Authenticated By   Authenticated On
-----
Total Entries: 0
```

Related Commands

Command	Description
clear aaa auth-survivability-cache	This command allows you to clear the data that is currently in the local Survival Server cache.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on stand-alone controller.

show aaa accounting tacacs

show aaa accounting tacacs

Description

This command displays TACACS+ data for your controller if you have previously configured a TACACS+ server and server group. The output includes the current TACACS+ accounting mode (enabled or disabled), and the name of the TACACS+ server group.

Example

The output of the `show aaa accounting tacacs` command displays configuration information for a TACACS+ accounting server. The output of this command includes the following parameters:

```
(host) #show aaa accounting tacacs
TACACS Accounting Configuration
-----
Parameter      Value
-----
Mode            Enabled
Commands       configuration
Server-Group   tacacs1
```

Parameter	Description
Mode	Shows whether this server group is Enabled or Disabled .
Commands	Displays the types of commands that are reported to the TACACS server group. <ul style="list-style-type: none">▪ action reports action commands only.▪ all reports all commands.▪ configuration reports configuration commands only▪ show reports show commands only
Server-Group	Shows whether this server is Enabled or Disabled .

Related Commands

Command	Description
aaa authentication-server tacacs	Configure the TACACS+ accounting feature.

Command	Description
aaa server-group	Add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa alias-group

show aaa alias-group [<ag_name>]

Description

This command shows an alias-group settings.

Parameter	Description
<ag_name>	Shows settings of specified alias-group.

Example

The following example shows the list of alias-groups:

```
(host) [mynode] #show aaa alias-group

Alias Group List
-----
Name   References  Profile Status
-----
default 2

Total:1
```

Related Commands

Command	Description
aaa alias-group	This command configures a AAA alias with set of VLAN derivation rules that could speed up user rule derivation processing for deployments with a very large number of UDRs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa authentication all

```
show aaa authentication all
```

Description

Show authentication statistics for your managed device, including authentication methods, successes and failures. This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive-portal, MAC or 801.X authentication profile, issue the commands specific to those features.

Example

The output of this command displays an authentication overview for your managed device, including the authentication methods used, and the numbers of successes or failures for each method. This example shows the numbers of authentication successes and failures for a managed device using TACACS+ and RADIUS authentication methods.

```
(host) #show aaa authentication all

Auth Method Statistics
-----
Method   Success  Failures
-----  -
tacacs   12       2 Radius
```

Related Commands

Command	Description
aaa authentication wispr	Configure WISPr authentication values on your Mobility Conductor.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa authentication captive-portal

```
show aaa authentication captive-portal [<profile-name>]
```

Description

This command shows configuration information for captive portal authentication profiles. Issue this command without the `<profile-name>` parameter to display the entire Captive Portal Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any captive portal authentication profiles defined, use the command [aaa authentication captive-portal](#) to configure your captive portal profiles.

Parameter	Description
<code><profile-name></code>	The name of an existing captive portal authentication profile.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a captive portal authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication captive-portal

Captive Portal Authentication Profile List
-----
Name           References  Profile Status
----           -
c-portal       2
remoteuser                    1
portall1                    1

Total: 4
```

Include a captive portal profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile `portall1`.

```
Captive Portal Authentication Profile "portall1"
-----
Parameter                               Value
-----
Default Role                             guest
```

```

Default Guest Role      guest
Server Group           default
Redirect Pause         10 sec
User Login             Enabled
Guest Login            Disabled
Logout popup window    Enabled
Use HTTP for authentication Disabled
Logon wait minimum wait 5 sec
Logon wait maximum wait 10 sec
logon wait CPU utilization threshold 60 %
Max Authentication failures 0
Show FQDN              Disabled
Authentication Protocol PAP
Login page             /auth/index.
Welcome page          /auth/welcom
Show Welcome Page     Yes
Add switch IP address in the redirection URL Disabled
Adding user vlan in redirection URL Disabled
Add a controller interface in the redirection URL N/A
Allow only one active user session Disabled
White List/Allow List N/A
Black List/Deny List  N/A
Show the acceptable use policy page Disabled
User idle timeout      N/A
Redirect URL           N/A
Bypass Apple Captive Network Assistant Disabled
URL Hash Key          *****

```

The output of this command includes the following parameters:

Parameter	Description
Default Role	Role assigned to the captive portal user upon login.
Default Guest Role	Guest role assigned to the captive portal user upon login.
Server Group	Name of the group of servers used to authenticate captive portal users.
Redirect Pause	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.
User Login	Shows whether the profile has enabled or disabled captive portal with authentication of user credentials.

Parameter	Description
Guest Login	Shows whether the profile has enabled or disabled captive portal guest login without authentication.
Logout popup window	Shows whether the profile has enabled or disabled a pop-up window that allows a user to log out. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station resets.
Use HTTP for authentication	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
Logon wait maximum wait	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
logon wait CPU utilization threshold	CPU utilization percentage above which the logon wait interval is applied when directing a captive portal user with the logon page.
Max Authentication failures	Maximum number of authentication failures before the user is blacklisted/denylisted.
Show FQDN	If enabled, the user can see and select the fully-qualified domain name (FQDN) on the captive portal login page.
Authentication Protocol	This parameter specifies the type of authentication required by this profile, PAP is the default authentication type.
Login page	URL of the page that appears for the user logon.
Welcome page	URL of the page that appears after logon and before the user is redirected to the web URL.

Parameter	Description
Add <code>controller</code> IP address in the redirection URL	If enabled, this option sends the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL.
Adding user <code>vlan</code> in redirection URL	Shows the user's VLAN ID sent in the redirection URL, if enabled
Add a <code>controller</code> interface in the redirection URL	Shows the IP address of a controller interface added to the redirection URL, if enabled.
Allow only one active user session	If enabled, only one active user session is allowed at any time. This feature is disabled by default.
White List/Allow List	Shows the configured whitelist/allowlist on an IPv4 or IPv6 network destination. The whitelist/allowlist contains authenticated websites that a guest can access.
Black List/Deny List	Shows the configured blacklist/denylist on an IPv4 or IPv6 network destination. The blacklist/denylist contains websites (unauthenticated) that a guest cannot access.
Show the acceptable use policy page	If enabled, the captive portal page will show the acceptable use policy page before the user logon page. This feature is disabled by default.
User Idle Timeout	The user idle timeout for this profile. The valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.
<code>redirect-url <url></code>	URL to which an authenticated user will be directed.
URL hash key	If this value is set, the redirection URL is hashed using the defined hash key. The characters in the hash key are hidden in the output of this command

Related Commands

Command	Description
aaa authentication captive-portal	This command is used to configure the parameters displayed in the output of this show command.

Command History

Version	Modification
ArubaOS 8.9.0.0	The following changes were introduced: All instances of <code>blacklist</code> have been replaced with <code>denylist</code> . All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa authentication captive-portal customization

show aaa authentication captive-portal customization <profile-name>

Description

Display customization settings for a captive portal profile. This command shows how a captive portal profile has been customized with non-default configuration settings. If you do not yet have any captive portal authentication profiles defined, use the command [aaa authentication captive-portal](#) to configure your captive portal profiles.

Parameter	Description
<profile-name>	The name of an existing captive portal authentication profile.

Example

The output of the following command shows how the captive portal profile *c-portal* has been customized. If an individual parameter has not been changed from its default settings, its value entry will be blank.

```
(host) #show aaa authentication captive-portal customization c-portal
Captive-Portal Customization
-----
Parameter                Value
-----
Login page design theme   3
Login page logo image
Login page text URL       /flash/upload/custom/ssu-guest-cp/logintext.html
Login policy text URL     /upload/custom/ssu-guest-cp/acceptableusepolicy.html
Custom page background color
Custom page background image /upload/custom/default/auth-slider-1.gif
```

The output of this command includes the following parameters:

Parameters	Description
Login page design theme	Indicates whether the controller is using one of the two predefined login page designs (1 or 2) or has a custom background (3).
Login page logo image	Path and filename for a custom captive portal logo. This option is only available if the controller has a predefined login design.
Login page text	Path and filename of the page that appears for the user logon.

Parameters	Description
Login policy text	Path and filename of the page that displays user policy text.
Custom page background color	Hexadecimal value for a custom background color. This option is only available if the controller has a custom login page design theme.
Custom page background image	Path and filename for a custom JPEG captive portal background image. This option is only available if the controller has a custom login page design theme.

Related Commands

Command	Description
aaa authentication captive-portal	This command is used to configure your captive portal profiles.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa authentication downloaded-cp-profiles

```
show aaa authentication downloaded-cp-profiles
```

Description

This command shows the downloaded CP profiles. Issue this command to display the entire downloaded CP profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Example

Include a captive portal profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal authentication profile cp2-d8941734:

```
Captive Portal Authentication Profile "cp2-d8941734"
-----
Parameter                               Value
-----
Default Role                             authenticated
Default Guest Role                       guest
Server Group                             cppm-rad-2
Redirect Pause                            10 sec
User Login                               Enabled
Guest Login                              Disabled
Logout popup window                      Enabled
Use HTTP for authentication              Disabled
Logon wait minimum wait                  5 sec
Logon wait maximum wait                  10 sec
logon wait CPU utilization threshold      60 %
Max Authentication failures                0
Show FQDN                                Disabled
Authentication Protocol                  PAP
Login page                               /auth/index.html
Welcome page                             /auth/welcome.html
Show Welcome Page                        Yes
Add switch IP address in the redirection URL Disabled
Adding user vlan in redirection URL       Disabled
Add a controller interface in the redirection URL N/A
Allow only one active user session        Disabled
White List                               N/A
Black List                               N/A
Show the acceptable use policy page       Disabled
User idle timeout                        -1
Redirect URL                             N/A
Bypass Apple Captive Network Assistant   Disabled
URL Hash Key                             *****

Total Downloaded CP profiles: 1
```

The output of this command includes the following parameters:

Parameter	Description
Default Role	Role assigned to the captive portal user upon login.
Default Guest Role	Guest role assigned to the captive portal user upon login.
Server Group	Name of the group of servers used to authenticate captive portal users.

Parameter	Description
Redirect Pause	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.
User Login	Shows whether the profile has enabled or disabled captive portal with authentication of user credentials.
Guest Login	Shows whether the profile has enabled or disabled captive portal guest login without authentication.
Logout popup window	Shows whether the profile has enabled or disabled a pop-up window that allows a user to log out. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station resets.
Use HTTP for authentication	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
logon wait maximum wait	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
Logon wait CPU utilization threshold	CPU utilization percentage above which the logon wait interval is applied when directing a captive portal user with the logon page.
Max Authentication failures	Maximum number of authentication failures before the user is blacklisted/denylisterd.
Show FQDN	If enabled, the user can see and select the fully-qualified domain name (FQDN) on the captive portal login page.
Authentication Protocol	This parameter specifies the type of authentication required by this profile, PAP is the default authentication type.

Parameter	Description
Login page	URL of the page that appears for the user logon.
Welcome page	URL of the page that appears after logon and before the user is redirected to the web URL.
Add controller IP address in the redirection URL	If enabled, this option sends the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL.
Adding user vlan in redirection URL	Shows the user's VLAN ID sent in the redirection URL, if enabled
Add a controller interface in the redirection URL	Shows the IP address of a controller interface added to the redirection URL, if enabled.
Allow only one active user session	If enabled, only one active user session is allowed at any time. This feature is disabled by default.
White List	Shows the configured white list on an IPv4 or IPv6 network destination. The white list contains authenticated websites that a guest can access.
Black List	Shows the configured black list on an IPv4 or IPv6 network destination. The black list contains websites (unauthenticated) that a guest cannot access.
Show the acceptable use policy page	If enabled, the captive portal page will show the acceptable use policy page before the user logon page. This feature is disabled by default.
User Idle Timeout	The user idle timeout for this profile. The valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.
redirect-url <url>	URL to which an authenticated user will be directed.

Parameter	Description
URL hash key	If this value is set, the redirection URL is hashed using the defined hash key. The characters in the hash key are hidden in the output of this command
Total Downloaded CP profiles	Shows the total number of downloaded CP profiles.

Related Commands

Command	Description
aaa authentication captive-portal	This command is used to configure the parameters displayed in the output of this show command.

Command History

Version	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa authentication dot1x

```
show aaa authentication dot1x [<profile-name>|countermeasures]
```

Description

This command shows information for 802.1X authentication profiles. Issue this command without the **<profile-name>** or **countermeasures** options to display the entire 802.1X Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed dot1x authentication configuration information for that profile. The **countermeasures** option indicates whether the 802.1X profiles have been configured for WPA/WPA2 countermeasures. If countermeasures have not been configured, the output for this command will be blank.

Parameter	Description
<profile-name>	The name of an existing 802.1X authentication profile.
countermeasures	Reports if WPA/WPA2 Countermeasures have been enabled for 802.1X profiles. If enabled, the AP scans for message integrity code (MIC) failures in traffic received from clients.

Examples

The following example lists all dot1x authentication profiles. The **References** column lists the number of other profiles with references to a 802.1X authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined 802.1X profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication dot1x

802.1X Authentication Profile List
-----
Name           References  Profile Status
-----
default        2
default-psk    1           Predefined (editable)
dot1x          5
dot1xtest      0

Total:4
```

To display a complete list of parameters for an individual profile, include the <profile> parameter. The example below displays some of the profile details for the authentication profile pDotix.

```
(host) #show aaa authentication dot1x pDot1x

802.1X Authentication Profile "pDot1x"
-----
Parameter                                     Value
-----
Max authentication failures                    0
Enforce Machine Authentication                Disabled
Machine Authentication: Default Machine Role  guest
Machine Authentication Cache Timeout          24 hrs
Blacklist/Denylist on Machine Authentication Failure Disabled
Machine Authentication: Default User Role     guest
Interval between Identity Requests           30 sec
Quiet Period after Failed Authentication      30 sec
Reauthentication Interval                     86400 sec
Use Server provided Reauthentication Interval Disabled
Multicast Key Rotation Time Interval          1800 sec
Unicast Key Rotation Time Interval           900 sec
...
```

The output of the **show aaa authentication dot1x** command includes the following parameters:

Parameter	Value
Max authentication failures	Number of times a user can try to login with wrong credentials after which the user is blacklisted /denylisted as a security threat. Blacklisting /Denylisting is disabled if this parameter is set to 0.

Parameter	Value
Enforce Machine Authentication	Shows if machine authentication is enabled or disabled for Windows environments. If enabled, if enabled, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.
Machine Authentication: Default Machine Role	Default role assigned to the user after completing only machine authentication.
Machine Authentication Cache Timeout	The timeout period, in hours, for machine authentication. After this period passes, the user will have to re-authenticate.
Blacklist/Denylist on Machine Authentication Failure	If enabled, the client is blacklisted /denylisted if machine authentication fails.
Machine Authentication: Default User Role	Default role assigned to the user after 802.1X authentication.
Interval between Identity Requests	Interval, in seconds, between identity request retries

Parameter	Value
Quiet Period after Failed Authentication	Interval, in seconds, following failed authentication.
Reauthentication Interval	Interval, in seconds, between reauthentication attempts.
Use Server provided Reauthentication Interval	If enabled, 802.1X authentication will use the server-provided reauthentication period.
Multicast Key Rotation Time Interval	Interval, in seconds, between multicast key rotations.
Unicast Key Rotation Time Interval	Interval, in seconds, between unicast key rotations.
Authentication Server Retry Interval	Server group retry interval, in seconds.
Authentication Server Retry Count	The number of server group retries.
Framed MTU	Shows the framed MTU attribute sent to the authentication server.
Number of times ID-Requests are retried	Maximum number of times ID requests are sent to the client.
Maximum Number of Reauthentication Attempts	Maximum number of reauthentication attempts.

Parameter	Value
Maximum number of times Held State can be bypassed	Number of consecutive authentication failures which, when reached, causes the controller to not respond to authentication requests from a client while the controller is in a held state after the authentication failure.
Dynamic WEP Key Message Retry Count	Number of times unicast/multicast EAPOL key messages are sent to the client.
Dynamic WEP Key Size	Dynamic WEP key size, either 40 or 128 bits.
Interval between WPA/WPA2 Key Messages	Interval, in milliseconds, between each WPA key exchange. The allowed range of values is 1000-5000 msec, and the default value is 1000 msec.
Delay between EAP-Success and WPA2 Unicast Key Exchange	Show the delay interval between EAP-Success and unicast key exchanges, in msec. Range: 0-2000msec. Default: 0 (no delay).

Parameter	Value
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	Interval, in milliseconds, between unicast and multicast key exchanges.
Time interval after which the PMKSA will be deleted	Show the PMKSA cache interval. Time interval in Hours. Range: 1-2000. Default: 8 hrs.
Delete Keycache upon user deletion Enabled	If enabled, the controller deletes the key cache entry when the user entry is deleted.
WPA/WPA2 Key Message Retry Count	Number of times WPA/WPA2 key messages are retried.
Multicast Key Rotation	Shows if multicast key rotation is enabled or disabled.
Unicast Key Rotation	Shows if unicast key rotation is enabled or disabled.
Reauthentication	If enabled, this option forces the client to do a 802.1X reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.)

Parameter	Value
Opportunistic Key Caching	If enabled, a cached pairwise master key (PMK) is derived with a client and an associated AP and used when the client roams to a new AP.
Validate PMKID	Shows if the Validate PMKID feature is enabled or disabled. When this option is enabled, the client must send a PMKID in the associate or reassociate frame to indicate that it supports OKC; otherwise, full 802.1X authentication takes place. (This feature is optional, since most clients that support OKC do not send the PMKID in their association request.)
Use Session Key	If enabled, the controller will use a RADIUS session key as the unicast WEP key.
Use Static Key	If enabled, the controller will use a static key as the unicast/multicast WEP key.
xSec MTU	Shows the size of the MTU for xSec.

Parameter	Value
Termination	Shows if 802.1X termination is enabled or disabled on the controller.
Termination EAP-Type	Shows the current Extensible Authentication Protocol (EAP) method, either EAP-PEAP or EAP-TLS.
Termination Inner EAP-Type	When EAP-PEAP is the EAP method, this parameter displays the inner EAP type.
Enforce Suite-B 128 bit or more security level Authentication	Shows if Suite-B 128 bit or more security level authentication enforcement is enabled or disabled.
Enforce Suite-B 192 bit security level Authentication	Shows if Suite-B 192 bit or more security level authentication enforcement is enabled or disabled.
Token Caching	If this feature enabled (and EAP-GTC is configured as the inner EAP method), token caching allows the controller to cache the username and password of each authenticated user.

Parameter	Value
Token Caching Period	Timeout period, in hours, for the cached information.
CA-Certificate	Name of the CA certificate for client authentication loaded in the controller.
Server-Certificate	Name of the Server certificate used by the controller to authenticate itself to the client.
TLS Guest Access	Shows if guest access for valid EAP-TLS users is enabled or disabled.
TLS Guest Role	User role assigned to EAP-TLS guest.
Ignore EAPOL-START after authentication	If enabled, the controller ignores EAPOL-START messages after authentication.
Handle EAPOL-Logoff	Shows if handling of EAPOL-LOGOFF messages is enabled or disabled.
Ignore EAP ID during negotiation	If enabled, the controller will ignore EAP IDs during negotiation.

Parameter	Value
WPA-Fast-Handover	Shows if WPA-fast-handover is enabled or disabled. This feature is only applicable for phones that support WPA.
Disable rekey and reauthentication for clients on call	Shows if the rekey and reauthentication features for voice-over-WLAN clients has been enabled or disabled.
Check certificate common name against AAA server	If enabled, this parameter verifies that the certificate's common name exists in the server. This parameter is disabled by default dot1x profiles.

Related Commands

Command	Description
aaa authentication dot1x	This command configures the 802.1X authentication profile.

Command History

Version	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication mac

```
show aaa authentication mac [<profile-name>]
```

Description

This command shows information for MAC authentication profiles. Issue this command without the

<profile-name> option to display the entire MAC Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed MAC authentication configuration information for that profile.

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows one MAC authentication profiles, **default**, which is referenced once by other profiles. the **Profile Status** column is blank, indicating that the profile is user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication mac

MAC Authentication Profile List
-----
Name       References  Profile Status
----       -
default    1

Total:1
```

The following example displays configuration details for the MAC authentication profile "default," including the delimiter and case used in the authentication request, and the maximum number of times a client can fail to authenticate before it is blacklisted/denylister.

```
(host) #show aaa authentication mac default
MAC Authentication Profile "default"
-----
Parameter                               Value
-----
Delimiter                                 none
Case                                       lower
Max Authentication failures               0
Reauthentication                         Disabled
```

```
Reauthentication Interval          86400 sec
Use Server provided Reauthentication Interval Disabled
```

Related Commands

Command	Description
aaa authentication mac	Configure MAC authentication values on your controller.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication mgmt

```
show aaa authentication mgmt
```

Description

This command displays administrative user authentication information, including management authentication roles and servers. Issue this command to identify the default management role assigned to authenticated administrative users, and the name of the group of servers used to authenticate these users.

Example

The output of the following example displays management authentication information for your controller.

```
(host) #show aaa authentication mgmt

Management Authentication Profile
-----
Parameter      Value
-----
Default Role   root
Server Group   ServerGroup1
Enable         Enabled
```

The output of the `show aaa authentication mgmt` command includes the following parameters:

Parameter	Description
Default Role	This parameter shows which of the following roles the controller uses for authentication management. <ul style="list-style-type: none">▪ root, the super user role (default).▪ guest-provisioning, guest provisioning role.▪ network-operations, network operator role.▪ read-only, read only role.▪ location-api-mgmt, location API management role.▪ no-access, no commands are accessible.
Server Group	The name of a server group.
Enable	The Enable parameter indicates whether or not this feature is enabled or disabled.

Related Commands

Command	Description
aaa authentication mgmt	Configure management authentication settings.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication stateful-ntlm

```
show aaa authentication stateful-ntlm [default|<profile-name>]
```

Description

This command shows the configuration settings of the stateful NT LAN Manager (NTLM) authentication profile. Issue this command without the <profile-name> parameter to display the entire stateful NTLM Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed Stateful NTLM authentication configuration information for that profile. Use this command to identify the default role assigned to users who have successfully authenticated using the NTLM authentication protocol, the name of the group of windows servers used to authenticate these users, and the NTLM authentication timeout period, in seconds.

Parameter	Description
default	Shows the configuration settings of the default NTLM authentication profile.
<profile-name>	Shows the configuration settings of the specified NTLM authentication profile.

Examples

The following example shows the configuration settings of the stateful NTLM authentication profile:

```
(host) [mynode] #show aaa authentication stateful-ntlm

Stateful NTLM Authentication Profile List
-----
Name                References  Profile Status
----                -
default             1
NTLMprofile1                1

Total:2
Two stateful NTLM authentication profiles, default and NTLMprofile1 are each
referenced once by other profiles. The blank Profile Status column indicates
that these profiles are both user-defined. If a profile is predefined, the
value Predefined appears in the Profile Status column.
The following example displays configuration details for the stateful NTLM
authentication profile "default".
(host) [node] #show aaa authentication stateful-ntlm default

Stateful NTLM Authentication Profile "default"
-----
```



```

Parameter      Value
-----      -
Default Role   guest
Server Group   default
Mode           Disabled
Timeout        10 sec

```

The output of this command includes the following parameters:

Parameter	Description
Default Role	This parameter shows the role assigned to NTLM authenticated users.
Server Group	The name of a windows server group.
Mode	The <code>Mode</code> parameter indicates whether or not this authentication profile is enabled or disabled.
Timeout	Timeout period for an authentication request, in seconds.

Related Commands

Command	Description
aaa authentication stateful-ntlm	This configures the settings displayed in the output of this show command.

Command History

Version	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication stateful-dot1x

```
show aaa authentication stateful-dot1x [config-entries]
```

Description

This command shows the stateful configuration settings of 802.1X authentication for clients on non-Aruba APs. Issue this command to identify the default role assigned to the 802.1X user group, name of the group of RADIUS servers used to authenticate the 802.1X users, and the 802.1X authentication timeout period in seconds.

Parameter	Description
config-entries	Display details for the AP Server configuration list.

Example

The following example shows the stateful configuration settings of 802.1X authentication information:

```
(host) [mynode] #show aaa authentication stateful-dot1x

Stateful 802.1X Authentication Profile
-----
Parameter      Value
-----
Default Role   guest
Server Group   newgroup2
Timeout        10 sec
Mode           Enabled
```

The output of this command includes the following parameters:

Parameter	Description
Default Role	This parameter shows which role the controller uses for 802.1X authentication management.
Server Group	The name of a server group.
Timeout	Timeout period for an authentication request, in seconds.
Mode	The Mode parameter indicates whether or not this feature is enabled or disabled.

Include the `config-entries` parameter to this command to show the AP - Server Configuration List.

```
(host) [mynode] #show aaa authentication stateful-dot1x config-entries

AP-Server Configuration List
-----
Cfg-Name          AP-IP          Server  Shared-Secret
-----          -
cfg22             10.3.14.6     RADIUS1 secret-pwd
```

The output of this command includes the following parameters:

Parameter	Description
Cfg-Name	is a auto-generated name
AP-IP	IP address of the AP.
Server	Name of the authentication server.
Shared-Secret	Shared authentication secret.

Related Commands

Command	Description
aaa authentication stateful-dot1x	This command configures a RADIUS server.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication stateful-kerberos

```
show aaa authentication stateful-kerberos [default|<profile-name>]
```

Description

This command shows the configuration settings of stateful Kerberos authentication profile.

Parameter	Description
default	Shows configuration settings of default Kerberos profile.
<profile-name>	Shows configuration settings of specified Kerberos profile name.

Example

The following example shows the configuration settings of the stateful Kerberos authentication profile:

```
(host) [mynode] #show aaa authentication stateful-kerberos
Stateful Kerberos Authentication Profile List
-----
Name      References  Profile Status
----      -
default  0

Total:1
The following example shows the configuration settings of the stateful
Kerberos authentication profile "default".
(host) [mynode] #show aaa authentication stateful-kerberos default

Stateful Kerberos Authentication Profile "default"
-----
Parameter      Value      Set
-----
Default Role    guest
Server Group    default
Timeout         10 sec
```

Related Commands

Command	Description
aaa authentication stateful-kerberos	This command configures stateful Kerberos authentication.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication via auth-profile

```
show aaa authentication via auth-profile [<profile-name>]
```

Description

This command displays configuration settings for the VIA Authentication profile. Issue this command without the **<profile-name>** option to display the entire VIA Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA authentication configuration information for that profile.

If you do not yet have any VIA authentication profiles defined, use the command [aaa authentication via auth-profile](#) to configure your VIA authentication profiles.

Parameter	Description
<profile-name>	The name of an existing VIA authentication profile.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via auth-profile

VIA Authentication Profile List
-----
Name       References  Profile Status
-----
default    0
via1       2
via2       1

Total:3
```

Include a VIA authentication profile name to display a complete list of configuration settings for that profile. The example below shows settings for the VIA authentication profile via1.

```
VIA Authentication Profile "via1"
-----
Parameter                               Value
-----
Default Role                             default-via-role
Server Group                             internal
Max Authentication failures               2
```

Description

VIA config for the MV office

The output of this command includes the following parameters:

Parameter	Description
Default Role	Role assigned to the captive portal user upon login.
Server Group	Name of the group of servers used to authenticate captive portal users.
Max Authentication failures	Maximum number of authentication failures before the user is blacklisted/denylisted.
Description	Description of the VIA authentication profile.

Related Commands

Command	Description
aaa authentication via auth-profile	This command configures the VIA authentication profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication via connection-profile

show aaa authentication via connection-profile [<profile-name>]

Description

This command displays configuration settings for the VIA connection profile. Issue this command without the <profile-name> option to display the entire VIA Connection profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA connection configuration information for that profile.

If you do not yet have any VIA connection profiles defined, use the command [aaa authentication via connection-profile](#) to configure your VIA connection profiles.

Parameter	Description
<profile-name>	The name of an existing VIA connection profile.

Examples

This first example shows that there are three configured connection profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA connection profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via connection-profile

VIA Connection Profile List
-----
Name           References  Profile Status
----           -
connection_1   3
connection_2   1
default        0

Total:3
```

Include a connection profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile connection_1.

```
VIA Connection Profile "default"
-----
Parameter                               Value
-----
VIA Servers                               N/A
Client Auto-Login                         Enabled
```



```

VIA Authentication Profiles to provision N/A
Allow client to auto-upgrade Enabled
VIA tunneled networks N/A
Enable split tunneling Disabled
VIA Client WLAN profiles N/A
Allow client side logging Enabled
VIA IKE V2 Policy Default
VIA IKE Policy Default
Use Windows Credentials Enabled
Use l2 forwarding Enabled
Enable IKEv2 Disabled
Use Suite B Cryptography Disabled
IKEv2 Authentication method user-cert
VIA IPsec V2 Crypto Map default-ikev2-
dynamicmap/10000
VIA IPsec Crypto Map default-
dynamicmap/10000
Allow user to save passwords Enabled
Enable Supplicant Disabled
Enable FIPS Module Disabled
Auto-launch Supplicant Disabled
Lockdown All Settings Disabled
Domain Suffix in VIA Authentication Disabled
Enable Controllers Load Balance Disabled
Enable Domain Pre-connect Enabled
VIA Banner Message Reappearance Timeout(minutes) 60
VIA Client Network Mask 255.255.255.255
Validate Server Certificate Enabled
VIA Client DNS Suffix List N/A
VIA max session timeout 1440 min
VIA Logon Script N/A
VIA Logoff Script N/A
VIA Support E-Mail Address N/A
Maximum reconnection attempts 3
VIA external download URL N/A
Allow user to disconnect VIA Enabled
Content Security Gateway URL N/A
Comma seperated list of HTTP ports to be inspected
(apart from default port 80) N/A
Enable Content Security Services Disabled
Keep VIA window minimized Disabled
Block traffic until VPN tunnel is up Disabled
Block traffic rules N/A

```

The output of this command includes the following parameters:

Parameter	Description
VIA servers	Displays the following information about the VIA server: <ul style="list-style-type: none"> <i>controller Hostname/IP Address</i>: This is the public IP address or the DNS hostname of the VIA controller. Users will connect to

Parameter	Description
	<p>remote server using this IP address or the hostname.</p> <ul style="list-style-type: none"> ▪ controller Internal IP Address: This is the IP address of any of the VLAN interface IP addresses belongs to this controller. ▪ controller Description: This is a human-readable description of the controller.
Client Auto-Login	<p>Enable or disable VIA client to auto login and establish a secure connection to the controller. Default: Enabled</p>
VIA Authentication Profiles to provision	<p>This is the list of VIA authentication profiles that will be displayed to users in the VIA client.</p>
Allow client to auto-upgrade	<p>Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the controller. Default: Enabled</p>
VIA tunneled networks	<p>A list of network destination (IP address and netmask) that the VIA client will tunnel through the controller. All other network destinations will be reachable directly by the VIA client.</p>
Enable split-tunneling	<p>Enable or disable split tunneling.</p> <ul style="list-style-type: none"> ▪ If enabled, all traffic to the VIA tunneled networks will go through the controller and the rest is just bridged directly on the client. ▪ If disabled, all traffic will flow through the controller. <p>Default: off</p>
Allow client-side logging	<p>Enable or disable client side logging. If enabled, VIA client will collect logs that can be sent to the support email-address for troubleshooting. Default: Enabled</p>
VIA Client WLAN profiles	<p>A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks.</p>
VIA IKEv2 Policy	<p>A list of IPsec crypto maps that the VIA client uses to connect to the controller. These IPsec Crypto Maps are configured in the CLI using the <code>crypto-local ipsec-map <ipsec-map-name></code> command.</p>

Parameter	Description
VIA IKE Policy	List of IKE policies that the VIA Client has to use to connect to the controller.
Use Windows Credentials	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO (Single Sign-on) feature can be utilized by remote users to connect to internal resources. Default: Enabled
Use l2 forwarding	Enable or disable the forwarding of Layer-2 GRE tunnel by VIA client.
Enable IKEv2	Select this option to enable or disable the use of IKEv2 policies for VIA.
Use Suite B Cryptography	Select this option to use Suite B cryptography methods. You must install the Advanced Cryptography license to use the Suite B cryptography.
IKEv2 Authentication method	List of all IKEv2 authentication methods.
VIA IPsec V2 Crypto Map	List of all IPsec V2 that the VIA client uses to connect to the controller.
VIA IPsec Crypto Map	List of IPsec Crypto Map that the VIA client uses to connect to the controller. These IPsec Crypto Maps are configured in CLI using the <code>crypto-local ipsec-map <ipsec-map-name></code> command.
Allow user to save passwords	Enable or disable users to save passwords entered in VIA. Default: Enabled
Enable Supplicant	If enabled, VIA starts in bSec mode using L2 suite-b cryptography. This option is disabled by default.
Enable FIPS Module	Shows if the VIA (Federal Information Processing Standard) FIPS module is enabled, so VIA checks for FIPS compliance during startup. This option is disabled by default.
Auto-Launch Supplicant	Select this option to automatically connect to a configured WLAN network.
Lockdown All Settings	If enabled, all user options on the VIA client are disabled.

Parameter	Description
Domain Suffix in VIA Authentication	Enables a domain suffix on VIA Authentication, so client credentials are sent as <i>domainname\username</i> instead of just <i>username</i> .
Enable controllers Load Balance	This option allows the VIA client to failover to the next available selected randomly from the list as configured in the VIA Servers option. If disabled, VIA will failover to the next in the sequence of ordered list of VIA Servers.
Enable Domain Pre-Connect	This option allows users with lost or expired passwords to establish a VIA connection to corporate network. This option authenticates the user's device and establishes a VIA connection that allows users to reset credentials and continue with corporate access.
VIA Banner Reappearance Timeout	The maximum time (in minutes) allowed before the VIA login banner reappears. Default: 1440 min
VIA Client Network Mask	The network mask that has to be set on the client after the VPN connection is established. Default: 255.255.255.255
Validate Server Certificate	Enable or disable VIA from validating the server certificate presented by the controller. Default: Enabled
VIA Client DNS Suffix List	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established. Default: None.
VIA max session timeout	The maximum time (minutes) allowed before the VIA session is disconnected. Default: 1440 min
VIA Logon Script	Name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside in the client computer.
VIA Logoff Script	Name of the log-off script that must be executed after the VIA connection is disconnected. The logoff script must reside in the client computer.
VIA Support E-mail Address	The support e-mail address to which VIA users will send client logs. Default: None.

Parameter	Description
Maximum reconnection attempts	The maximum number of re-connection attempts by the VIA client due to authentication failures. Default: 3
VIA external download URL	End users will use this URL to download VIA on their computers.
Allow user to disconnect VIA	Enable or disable users to disconnect their VIA sessions. Default: Enabled
Content Security Gateway URL	If split-tunnel forwarding is enabled, access to external (non-corporate) web sites will be verified by the specified content security service provider.
Comma Separated List of HTTP Ports	Traffic from the specified ports will be verified by the content security service provider.
Enable Content Security Services	Select this check box to enable content security service. You must install the Content Security Services licenses to use this option.
Keep VIA window minimized	Enable this option to minimize the VIA client to system tray during the connection phase. Applicable to VIA client installed in computers running Microsoft Windows operating system.
Block traffic until VPN tunnel is up	If enabled, this feature will block network access until the VIA VPN connection is established.
Block traffic rules	Specify a hostname or IP address and network mask to define a whitelist/allowlist of users to which the Block traffic until VPN tunnel is up setting will not apply.

Related Commands

Command	Description
aaa authentication via connection-profile	This command is used to configure the parameters displayed in the output of this show command.

Command History

Version	Modification
ArubaOS 8.4.0.0	The Use 12 forwarding parameter was added to the output of the show aaa authentication via connection-profile command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication via global-config

show aaa authentication via global-config

Description

This command shows the VIA global configuration.

Example

The following example shows the VIA global configuration:

```
(host) [mynode] #show aaa authentication via global-config

VIA Global Configuration
-----
Parameter                               Value
-----
Allow VIA SSL Fallback                   Enabled
Max Concurrent VIA VPN Sessions per user 5
```

Related Commands

Command	Description
aaa authentication via global-config	This command allows you to enable SSL fallback mode.

Command History

Release	Modification
ArubaOS 8.11.0.0	The command output displays the maximum number of concurrent VIA VPN sessions allowed per user.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor or managed devices.

show aaa authentication via web-auth

```
show aaa authentication via web-auth [default]
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (<https://<server-IP-address>/via>) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Issue this command to view the authentication profiles associated with the default web authentication profile. Use it without the profile name to see the list of authentication profiles.

Examples

```
(host) #show aaa authentication via web-auth

VIA Web Authentication List
-----
Name       References  Profile Status
----       -
default    2

Total:1

(host) #show aaa authentication via web-auth default

VIA Web Authentication "default"
-----
Parameter                               Value
-----
VIA Authentication Profiles             vial
```

The output of this command includes the following parameters:

Parameter	Description
VIA Authentication Profiles	This is the name of the VIA authentication profile. The value column displays the order of priority in which the profiles are displayed in the VIA client login.

Related Commands

Command	Description
aaa authentication via web-auth	The web authentication profile is used by end users to login to the VIA download page (<i>https://<server-IP-address>/via</i>) for downloading the VIA client.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication vpn

```
show aaa authentication vpn [default|default-cap|default-rap]
```

Description

This command displays VPN authentication settings, including authentication roles and servers. Issue this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted/denylisted.

Example

The following example displays configuration details for the VPN authentication profile **default**, **default-cap** and **default-rap**.

```
(host) #show aaa authentication vpn default

VPN Authentication Profile "default"
-----
Parameter                               Value
-----
Default Role                             default-vpn-role
Server Group                             default
RADIUS Accounting Server Group           N/A
Max Authentication failures               0
Check certificate common name against AAA server Enabled
Export VPN IP address as a route         Enabled
User idle timeout                         N/A
PAN Firewall Integration                  Disabled

(TechPubs) #show aaa authentication vpn default-cap

VPN Authentication Profile "default-cap" (Predefined (changed))
-----
Parameter                               Value
-----
Default Role                             sys-ap-role
Server Group                             internal
RADIUS Accounting Server Group           N/A
Max Authentication failures               0
Check certificate common name against AAA server Enabled
Export VPN IP address as a route         Enabled
User idle timeout                         N/A
PAN Firewall Integration                  Disabled

(TechPubs) #show aaa authentication vpn default-rap

VPN Authentication Profile "default-rap" (Predefined (changed))
-----
Parameter                               Value
```

```

-----
Default Role                               default-vpn-role
Server Group                               default
RADIUS Accounting Server Group            N/A
Max Authentication failures                0
Check certificate common name against AAA server Enabled
Export VPN IP address as a route          Enabled
User idle timeout                          N/A
PAN Firewall Integration                   Disabled

```

Parameter	Description
Default Role	The default role to be assigned to VPN users.
Server Group	The name of the server group that performs the authentication.
RADIUS Accounting Server Group	The name of the RADIUS accounting server group.
Max Authentication failures	Number of times a user attempted to authenticate, but failed.
Check certificate common name against AAA server	When enabled, this parameter triggers a validation against the configured AAA server.
Export VPN IP address as a route	When enabled, any VPN client address is exported to OSPF using IPC.
User idle timeout	The amount of time in minutes that a user can be inactive before the user's session times out and closes.
PAN Firewall Integration	Integration with existing Palo Alto Networks (PAN) firewalls policy.

Related Commands

Command	Description
aaa authentication via auth-profile	This command configures the VIA authentication profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication wired

```
show aaa authentication wired
```

Description

View wired authentication settings for a client device that is directly connected to a port on the controller. This command displays the name of the AAA profile currently used for wired authentication.

Example

The following example shows the current wired profile for the controller is a profile named default.

```
(host) #show aaa authentication wired
Wired Authentication Profile
-----
Parameter      Value
-----
AAA Profile    default
Denylist-time  3600 sec
```

Related Commands

Command	Description
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication wispr

```
show aaa authentication wispr <profile-name>
```

Description

This command shows information for a WISPr authentication profiles. Issue this command without the **<profile-name>** option to display the entire WISPr Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed WISPr authentication configuration information for that profile.

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows two WISPr authentication profiles, **default** and **WISPr1**, which are referenced two times by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication wispr

WISPr Authentication Profile List
-----
Name           References  Profile Status
-----
default        2
WISPr1 2
Total:2
```

The following example displays configuration details for the WISPr authentication profile "default".

```
(host) ##show aaa authentication wispr default

WISPr Authentication Profile "default"
-----
Parameter                               Value
-----
Default Role                             guest
Server Group                             default
Max Authentication failures              0
```

```

User Agent String          N/A
Logon wait minimum wait   5 sec
Logon wait maximum wait   10 sec
logon wait CPU utilization threshold 60 %
WISPr Location-ID ISO Country Code N/A
WISPr Location-ID E.164 Country Code N/A
WISPr Location-ID E.164 Area Code N/A
WISPr Location-ID SSID/Zone N/A
WISPr Operator Name       N/A
WISPr Location Name       N/A

```

The output of this command includes the following parameters:

Parameter	Description
Default Role	The default role assigned to users that have completed WISPr authentication.
Server Group	The name of the server group that performs the authentication.
Max Authentication failures	Displays the number of maximum auth failures before user is denylisted.
User Agent String	Displays the user agent string registered for use in WISPR Profile.
Logon wait minimum wait	If the controller's CPU utilization has surpassed the Logon wait CPU utilization threshold value , the <code>Logon wait minimum wait</code> parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
Logon wait maximum wait	If the controller's CPU utilization has surpassed the logon wait CPU utilization threshold value , the <code>Logon wait maximum wait</code> parameter defines the maximum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
WISPr Location-ID E.164 Area Code	The E.164 Area Code in the WISPr Location ID.
WISPr Location-ID E.164 Country Code 1	The 1-3 digit E.164 Country Code in the WISPr Location ID.

Parameter	Description
WISPr Location-ID ISO Country Code	The ISO Country Code in the WISPr Location ID.
WISPr Location-ID SSID/Zone	The SSID/network name in the WISPr Location ID.
WISPr Location Name	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
WISPr Operator Name	A name identifying the hotspot operator.

Related Commands

Command	Description
aaa authentication wispr	Configure WISPr authentication values on your Mobility Conductor.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication-server all

```
show aaa authentication-server all
```

Description

View authentication server settings for both external authentication servers and the internal controller database. The output of this command displays statistics for the Authentication Server Table, including the name and address of each server, server type and configured authorization and accounting ports.

Example

The following command shows information for the internal Authentication server, and another RADIUS server named RADIUS-1.

```
(host) #show aaa authentication-server all

Auth Server Table
-----
Name   Type  FQDN  IP addr  AuthPort  AcctPort  Status  Requests
-----
Internal Local n/a  10.4.62.11 n/a   n/a   Enabled  0
server  Ldap  n/a  0.0.0.0  389   n/a   Enabled  0
server  Radius SRVR1 127.9.9.61 1812  1813  Enabled  0
default Tacacs n/a  127.9.10.61 49    n/a   Enabled  0
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the authentication server.
Type	The type of authentication server. ArubaOS supports LDAP, RADIUS and TACACS+ servers, in addition to its own local, internal authentication server.
FQDN	The Fully-Qualified Domain Name of the server, if configured.
IP addr	IP address of the server, in dotted-decimal format.
AuthPort	Port number used for authentication. An LDAP server uses port 636 for LDAP over SSL, and port 389 for SSL over LDAP, Start TLS operation and clear text. The default RADIUS authentication port is port 1812.

Parameter	Description
AcctPort	Accounting port on the server. The default RADIUS accounting port is port 1813.
AcctPort	Accounting port on the server.
Status	Shows whether the Authentication server is enable or disabled.
Requests	Number of authentication requests received by the server.

Related Commands

Command	Description
aaa authentication-server internal	This command specifies that the internal database on a managed device be used for authenticating clients.
aaa authentication-server ldap	This command configures an LDAP server.
aaa authentication-server radius	This command configures a RADIUS server.
aaa authentication-server tacacs	This command configures a TACACS+ server.
aaa authentication-server windows	This command configures a windows server for stateful-NTLM authentication.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication-server internal

```
show aaa authentication-server internal [statistics]
```

Description

View authentication server settings for the internal controller database.

Examples

The output of the command below shows that the internal authentication server has been disabled:

```
(host) #show aaa authentication-server internal

Internal Server
-----
Host   IP addr   Retries Timeout Status
-----
Internal 10.168.254.221 3    5    Disabled
```

The following data columns appear in the output of this command:

Parameter	Description
Host	Name of the internal authentication server.
IP addr	Address of the internal server, in dotted-decimal format.
Retries	Number of retries allowed before the server stops attempting to authenticate a request.
Timeout	Timeout period, in seconds.
Status	Shows if the server is enabled or disabled

Include the `statistics` parameter to display additional details for the internal server.

```
(host) #show aaa authentication-server internal statistics

Internal Database Server Statistics
-----
PAP Requests           8
PAP Accepts            8
PAP Rejects            0
MSCHAPv2 Requests     0
MSCHAPv2 Accepts      0
```

```

MSCHAPv2 Rejects      0
Mismatch Response     0
Users Expired         1
Unknown Response      0
Timeouts              1
AvgRespTime (ms)     0
Uptime (d:h:m)       4:3:32
SEQ first/last/free  1,255,255

```

The following data columns appear in the output of this command:

Parameter	Description
PAP Requests	Number of PAP requests received by the internal server.
PAP Accepts	Number of PAP requests accepted by the internal server.
PAP Rejects	Number of PAP requests rejected by the internal server.
MSCHAPv2 Requests	Number of MSCHAPv2 requests received by the internal server.
MSCHAPv2 Accepts	Number of MSCHAPv2 requests accepted by the internal server.
MSCHAPv2 Rejects	Number of MSCHAPv2 requests rejected by the internal server.
Mismatch Response	Number of times the server received an authentication response to a request after another request had been sent.
Users Expired	Number of users that were deauthenticated because they stopped responding.
Unknown Response	Number of times the server did not recognize the response, possibly due to internal errors.
Timeouts	Number of times that the controller timed out an authentication request.
AvgRespTime (ms)	Time it takes the server to respond to an authentication request, in seconds.
Uptime (d:h:m)	Time elapsed since the last server reboot.
SEQ first/last/free	This internal buffer counter keeps track of the requests to the authentication server.

Related Commands

Command	Description
aaa authentication-server internal	This command specifies that the internal database on a managed device be used for authenticating clients.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication-server ldap

```
show aaa authentication-server ldap [statistics|<ldap_server_name> status]
```

Description

This command shows the configuration settings of LDAP servers.

Parameter	Description
statistics	Shows the statistics of all LDAP servers.
<ldap_server_name> status	Shows the status of the specified LDAP server.

Examples

The following example shows the LDAP server list with the names of all the LDAP servers:

```
(host) [mynode] #show aaa authentication-server ldap

LDAP Server List
-----
Name   References  Profile Status
----  -
ldap1  5
ldap2  3
ldap3  1

Total:3
```

The **References** column lists the number of other profiles that reference an LDAP server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

Related Commands

Command	Description
aaa authentication-server ldap	This command configures an LDAP server.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa authentication-server radius

```
show aaa authentication-server radius [statistics|<rad_server_name> radsec status]
```

Description

This command shows the configuration settings of RADIUS servers.

Parameter	Description
statistics	Shows the statistics of all RADIUS servers.
<rad_server_name> radsec status	Shows status of RADIUS over TLS of specified RADIUS server.

Examples

The following example shows the RADIUS server list with the names of all the RADIUS servers:

```
(host) [mynode] #show aaa authentication-server radius

RADIUS Server List
-----
Name           References  Profile Status
----           -
myserver       3
radius         0
servername     0

Total:3
```

The **References** column lists the number of other profiles that reference a RADIUS server, and the **Profile Status** column indicates whether the profile is predefined. User-defined servers will not have an entry in the **Profile Status** column.

Include the optional `statistics` parameter to this command to show the following statistics for all RADIUS servers:

Parameter	Description
Server	Name of the RADIUS server.
Acct Rq	Accounting requests. This reports of the number of accounting messages (for example, start/stop/interim update) sent by the controller to a RADIUS server. This counter increments whenever the controller sends one of these messages.

Parameter	Description
Raw Rq	Raw requests. Number of raw authentication requests the controller sent to a RADIUS server.
PAP Rq	Pap Requests. Number of PAP authentication requests the controller sent to a RADIUS server.
CHAP Rq	CHAP requests. Number of CHAP authentication requests the controller sent to a RADIUS server.
MSCHAP Rq	MSCHAP requests. Number of MS-CHAP authentication requests the controller sent to a RADIUS server.
MSCHAPv2 Rq	MSCHAPv2 requests. Number of MS-CHAPv2 requests the controller sent to a RADIUS server.
Mismatch Rsp	Mismatch responses. Number of responses from a RADIUS server for which the controller does not have the proper request context.
Bad Auth	Bad authenticator. Number of responses from the RADIUS server with an invalid secret or bad reply digest.
Acc	Access accept. Number of responses from the RADIUS server that indicate that client authentication succeeded.
Rej	Access reject. Number of responses from the RADIUS server that indicate that client authentication failed.
Acct Rsp	Accounting response. Number of responses sent from the RADIUS server in response to accounting requests sent from the controller.
Chal	Access challenge. Number of responses from the RADIUS server containing a challenge for the client (to complete authentication).
Ukn Rsp	Unknown Response code. Number of responses from the RADIUS server that were not understood by the controller due to the purpose or type of the response
Tmout	Timeouts. Number of messages sent by the controller for which the controller did not receive a response before the message timed out. NOTE: Timeouts include RADIUS accounting requests. Every request controller sends to the RADIUS server is monitored for a timeout, so each retry increments this counter.
AvgRspTme	Average response time. Time taken, on an average, for the RADIUS server to respond to a message from the controller.

Parameter	Description
Tot Rq	Total errors. This counter reflects the total number of requests sent to the RADIUS server (auth and accounting requests).
Tot Rsp	This counter reflects the total number of responses received by the RADIUS server (auth and accounting responses).
Rd Err	Read errors. This counter reflects the total number of errors encountered while reading off socket corresponding to that RADIUS server.
Uptime	Amount of for which the RADIUS server has been active/up. The RADIUS server is considered to have an UP status if the server is active and serving requests. The RADIUS server is considered to be DOWN if the server is not responding. For example, if the RADIUS server does not respond for (<no of retries> * < timeout>) seconds, the controller takes the RADIUS server down. It brings the radius server back into service after the dead timeout.
SEQ	Information corresponding to the sequence number of requests. SEQ total corresponds to the total number of sequence numbers that can be used to communicate with the RADIUS server. SEQ free corresponds to the free/available/not in use sequence numbers for a particular RADIUS server.

The following example shows additional details for a RADIUS server named alpha:

```
(host) [mynode] #show aaa authentication-server radius alpha

RADIUS Server "alpha"
-----
Parameter                               Value
-----
Host                                     10.15.28.101
Key                                     *****
CPPM credentials                         ade/*****
Auth Port                               1812
Acct Port                               1813
Radsec Port                             2083
Retransmits                             3
Timeout                                 5 sec
NAS ID                                  N/A
NAS IP                                   N/A
Enable IPv6                             Disabled
NAS IPv6                                 N/A
Source Interface                         N/A
Use MD5                                  Disabled
Use IP address for calling station ID    Disabled
Mode                                     Enabled
Lowercase MAC addresses                  Disabled
MAC address delimiter                    none
```

```

Service-type of FRAMED-USER      Disabled
Radsec                           Enabled
Radsec Trusted CA Name          can-new
Radsec Server Cert Name         N/A
Radsec Client Cert              client-new
called-station-id               macaddr colon disable

```

The output of this command includes the following information:

Parameter	Description
Host	IP address of the RADIUS server
Key	Shared secret between the controller and the authentication server.
CPPM credentials	Setting this parameter allows the controller to use configurable username and password instead of a support password.
Auth port	Authentication port on the server.
Acct Port	Accounting port on the server.
Radsec Port	Displays the Radsec port for RADIUS data transport.
Retransmits	Maximum number of retries sent to the server by the controller before the server is marked as down.
Timeout	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
NAS ID	Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP	NAS IP address to send in RADIUS packets. If you do not configure a server-specific NAS IP, the global NAS IP is used.
Enable IPv6	Shows if the RADIUS server is enabled in IPv6 mode.
NAS IPv6	IPv6 address for the global NAS IP which the controller uses to communicate with all the RADIUS servers.
Source Interface	The source interface VLAN ID number.

Parameter	Description
Use MD5	If enabled, the RADIUS server will use a MD5 hash of cleartext password.
Use IP address for calling station ID	If enabled, the RADIUS server will use an IP address instead of a MAC address for calling station IDs.
Mode	Shows whether this server is Enabled or Disabled .
Lowercase MAC addresses	If this feature is enabled, the server will send MAC addresses in lowercase letters.
MAC address delimiter	The character used as a MAC address delimiter. If no character is specified, the RADIUS server will use a colon (:) by default.
Service-type of FRAMED-USER	If this option is enabled, the server sends the service-type as FRAMED-USER instead of LOGIN-USER. This option is disabled by default
Radsec	Displays the status of the Radsec server.
Radsec Trusted CA	Displays the Certificate Authority to sign Radsec certificates.
Radsec Server Cert Name	Displays the trusted Radsec server certificate.
Radsec Client Cert	Displays the Radsec client certificate on the RADIUS server that identifies and authenticates clients.
called-station-id	Configure this parameter to be sent with the RADIUS attribute Called Station ID for authentication and accounting requests. The <code>called-station-id</code> parameter can be configured to include AP group, AP MAC address, AP name, controller IP, controller MAC address, or user vlan. The default value is controller MAC address.

The following example shows details of RADIUS over TLS for a RADIUS server named beta:

```
(host) [mynode] #show aaa authentication-server radius <servername> radsec
status

Radius Server "beta" Radsec Status
-----
Radsec Server Attribute  Value
-----
In Service                Yes
```

Connected Sockets

1

The output of this command includes the following information:

Parameter	Description
In Service	Shows the status of the Radsec RADIUS server.
Connected Sockets	Shows the number of TLS connections with the RADIUS server.

Related Commands

Command	Description
aaa authentication-server radius	This command configures a RADIUS server.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication-server tacacs

```
show aaa authentication-server tacacs [<tacacs_server_name>]|statistics
```

Description

Display configuration settings for your TACACS+ servers.

Parameter	Description
<tacacs_server_name>	Name that identifies an TACACS+ server.
statistics	Displays accounting, authorization, and authentication request and response statistics for the TACACS server.

Examples

The output of the example below displays the TACACS+ server list with the names of all the TACACS+ servers. The **References** column lists the number of other profiles that reference a TACACS+ server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server tacacs

TACACS Server List
-----
Name                References  Profile Status
-----
LabAuth              5
TACACS1              3

Total:2
```

Include the <tacacs_server_name> parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server tacacs tacacs1

TACACS Server "tacacs1"
-----
Parameter    Value
-----
Host          10.1.1.16
Key           *****
TCP Port      49
Retransmits   3
Timeout       20 sec
```

Mode Enabled

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the TACACS+ server
Key	Shared secret between the controller and the authentication server.
TCP Port	TCP port used by the server.
Retransmits	Maximum number of retries sent to the server by the controller before the server is marked as down.
Timeout	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
Mode	Shows whether this server is Enabled or Disabled .

Related Commands

Command	Description
aaa authentication-server tacacs	This command configures a TACACS+ server.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa authentication-server windows

```
show aaa authentication-server windows [<windows_server_name>]
```

Description

Display configuration settings for your Windows servers.

Parameter	Description
<windows_server_name>	Name that identifies a Windows server.

Examples

The output of the example below displays the Windows server list with the names of all the Windows servers used for NTLM authentication. The **References** column lists the number of other profiles that reference a Windows server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server windows

Windows Server List
-----
Name                References  Profile Status
----                -
NTLM                 1
Windows2            1

Total:2
```

Include the <windows_server_name> parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server windows Windows2

Windows Server "windows"
-----
Parameter          Value
-----
Host                172.21.18.170
Mode                Enabled
Windows Domain     MyCompanyDomain
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the Windows server
Mode	Shows whether this server is Enabled or Disabled .
Windows Domain	Name of the Windows domain to which this server is assigned.

Related Commands

Command	Description
aaa authentication-server windows	This command configures a windows server for stateful-NTLM authentication.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa bandwidth-contracts

```
show aaa bandwidth-contracts [dynamic | name]
```

Description

This command shows the contract names, ID numbers, Rate limits, and Note for your bandwidth contracts.

Parameter	Description
dynamic	Displays dynamic bandwidth contracts.
name	Displays the bandwidth contract for the name specified.

Example

Specify a bandwidth contract name to view information for a specific bandwidth contract, or omit that parameter to view information for all bandwidth contracts configured . The output of the following command shows that the bandwidth contract **VLAN** has a configured rate of 6 Mbps, and the contract **User** has a rate of 2048 Kbps.

```
(host) #show aaa bandwidth-contracts VLAN

Bandwidth Contract
-----
Contract      Id  Rate (bits/second)
-----
VLAN          1   6000000
User          2   2048000

Total contracts = 2
Per-user contract total = 4096
Per-user contract usage = 0
```

Execute the following command to view the dynamic bandwidth contracts:

```
(host) #show aaa bandwidth-contracts dynamic

Dynamic Bandwidth Contracts
-----
Contract                                     Id  Rate           Note
-----
"$#-DBW-0000000004-UP"                       3   2000000 bps   Group(1)
"$#-DBW-0000000004-DN"                       4   1000000 bps   Group(1)
"$#-DBW-44:00:00:00:00:02-UP"                 5   5000000 bps   Individual
"$#-DBW-44:00:00:00:00:02-DN"                 6   6000000 bps   Individual
"$#-DBW-44:00:00:00:00:03-UP"                 7   5000000 bps   Individual
```

```
"$#-DBW-44:00:00:00:00:03-DN" 8 6000000 bps Individual
Total Instances: 6
```

Related Commands

Command	Description
aaa bandwidth-contract	Use this command to define contracts to limit traffic for a user or VLAN.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>dynamic</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show aaa cluster essid

```
show aaa cluster essid <ssid_val>
```

bucketmap	all buckets in cluster essid table
counters	display bucket counters
keycache	keycache
mac	Match macaddr
users	all users

Description

This command displays information on essid counters, bucketmap, dormant keycache, mac address, and dormant user entries for a particular ESSID.

Parameter	Description
bucketmap	Displays the bucketmap details for a specified bucket.
counters	Displays all the bucket counters.
keycache [standby]	Displays the dormant keycache entries.
users [standby]	Displays all user entries in dormant hash table.
mac	Displays the match mac address

Example

The output of the example below displays the bucketmap details and the counters for the essid, Zone1TestEssid:

```
show aaa cluster essid Zone1TestEssid bucketmap bucket 2
```

```
(host) (config) #show aaa cluster essid Zone1TestEssid bucketmap bucket 2

Active Bucket Values
-----
Essid      Bucket  ActiveUAC   StandbyUAC   L2Conn  IS_Active  IS_
Standby
-----
Zone1TestEssid 2      10.15.146.5 10.15.146.4 1        0          0
show aaa cluster essid Zone1TestEssid counters
(host) (config) #show aaa cluster essid Zone1TestEssid counters

Counters for ESSID: Zone1TestEssid
Bucketmap essid create.....1
Total Bucketmap updates.....1
```

```
Last update reason .....0
Last update time ..... Fri Jun 17 12:24:18 2016
```

Related Commands

Command	Description
show aaa cluster essid-all	This command displays all active essid entries in essid hash table. That is, it displays information on essid counters, bucketmap, dormant keycache, and dormant user entries.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on managed devices.

show aaa cluster essid-all

```
show aaa cluster essid-all
  bucketmap
  counters
  keycache
  users
```

Description

Displays all active essid entries in essid hash table. That is, it displays information on essid counters, bucketmap, dormant keycache, and dormant user entries.

Parameter	Description
bucketmap	Displays the bucketmap details for a specified bucket.
counters	Displays all the bucket counters.
keycache [standby]	Displays the dormant keycache entries.
users [standby]	Displays all user entries in dormant hash table.

Example

The output of the example below displays the bucketmap details and the counters for a particular ESSID:

```
show aaa cluster essid-all bucketmap bucket 2
```

```
(host) (config) #show aaa cluster essid-all bucketmap bucket 2
Active Bucket Values
-----
Essid          Bucket  ActiveUAC   StandbyUAC   L2Conn  IS_Active  IS_Sta
-----
              ndby
-----

Zone1TestEssid 2          10.15.146.5  10.15.146.4  1        0          0
show aaa cluster essid-all counters
(host) (config) #show aaa cluster essid-all counters
Global Cluster Counters:
Cluster Enabled.....2
Cluster Disabled.....2
BucketMap Add.....11
BucketMap Del.....6
Macuser Dormant Evts.....2
Macuser Dormant Add.....1
```

```

Macuser Dormant Delete.....1
IPuser Dormant Evt.....2
IPuser Dormant Add.....1
IPuser Dormant Delete.....1
STA dormant del to SOS.....1
STA dormant create to SOS.....1
STA dormant IP create to SOS...1
STA dormant send keys to SOS...1
Total Bucketmap updates for the system : 11
Counters for ESSID: Srinizone1TestEssid
Bucketmap essid create.....1
Total Bucketmap updates.....1
Last update reason .....0
Last update time ..... Fri Jun 17 12:24:18 2016

```

Related Commands

Command	Description
show aaa cluster essid	This command displays information on essid counters, bucketmap, dormant keycache, mac address, and dormant user entries for a particular ESSID.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show aaa cluster gsm macuser-section mac

```
show aaa cluster gsm macuser-section mac <macaddr>
```

Description

This command displays gsm mac user section for a particular MAC address.

Parameter	Description
macaddr	Displays the gsm mac user section for the specified MAC address.

Related Commands

Command	Description
show aaa cluster gsm ipuser-section	This command displays gsm ip user section for a particular IP address.
show aaa cluster gsm user-section	This command displays gsm user section.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show aaa cluster gsm ipuser-section

```
show aaa cluster gsm ipuser-section {ip <ipaddr> | ipv6 <ipv6-addr>}
```

Description

This command displays gsm ip user section for a particular IP address.

Syntax

Parameter	Description
ipaddr	Displays the gsm ip user section for the specified IP address.
ipv6-addr	Displays the gsm ip user section for the specified IPv6 address.

Related Commands

Command	Description
show aaa cluster gsm macuser-section mac	This command displays gsm mac user section for a particular MAC address.
show aaa cluster gsm user-section	This command displays gsm user section.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ipv6-addr</code> sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show aaa cluster gsm user-section

show aaa cluster gsm user-section <uuid>

Description

This command displays gsm user section.

Syntax

Parameter	Description
uuid	Enter user uuid in hex.

Related Commands

Command	Description
show aaa cluster gsm macuser-section mac	This command displays gsm mac user section for a particular MAC address.
show aaa cluster gsm ipuser-section	This command displays gsm ip user section for a particular IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show aaa cluster member

```
show aaa cluster member
```

Description

Displays all the cluster members with their IP address and the current cluster state.

Example

The output of the example below displays the cluster members.

```
(host) (config) #show aaa cluster members

Current Cluster State: ENABLED, Count: Enabled(2), Disabled(2)
-----
Cluster  IP            NASip
-----  --            -
Self     10.15.146.3    0.0.0.0
Peer     10.15.146.4    0.0.0.0
Peer     10.15.146.5    0.0.0.0
Peer     10.15.146.6    0.0.0.0
```

Related Commands

Command	Description
lc-cluster group-membership	Configure the group-membership in each node. This command is used to enable the cluster membership on the managed devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show aaa debug

```
show aaa debug
  age {dev-id-cache [mac <A:B:C:D:E:F>]|key-cache [mac <A:B:C:D:E:F>]|pmk-cache
    [mac <A:B:C:D:E:F>]}
  dev-id-cache
  pmk bss-table [<A:B:C:D:E:F>]
  role user {ip <A.B.C.D>|ipv6 <ipv6addr>|mac <A:B:C:D:E:F>}
  stm
  vlan user {ip <A.B.C.D>|ipv6 <ipv6addr>|mac <A:B:C:D:E:F>}
```

Description

This command shows AAA related debug information.

Parameter	Description
age dev-id-cache key-cache pmk-cache	Displays the age of the GSM entry since the previous refresh (in seconds) based on: <ul style="list-style-type: none">▪ dev-id-cache—Device ID information in memory.▪ key-cache—Key cache information in memory.▪ pmk-cache—Pairwise Master Key (PMK) cache information in memory.
dev-id-cache section mac <mac address>	Displays Device Id cache section CPPM information in memory.
pmk bss-table	Displays PMK related debug information based on the BSSID address.
role user ip ipv6 mac	Displays role derivation related debug information based on: <ul style="list-style-type: none">▪ ip—IPv4 address of the client.▪ ipv6—IPv6 address of the client.▪ mac—MAC address of the client.
stm message stats	Displays information about number of messages sent or received from stm.
vlan user ip ipv6 mac	Displays VLAN derivation related debug information based on: <ul style="list-style-type: none">▪ ip—IPv4 address of the client.▪ ipv6—IPv6 address of the client.▪ mac—MAC address of the client.

Example

The following example shows the VLAN derivation debug information of an user with IPv4 address.

```
(host) [mynode] #show aaa debug vlan user ip 192.0.2.1

VLAN types present for this User
=====
Default VLAN                : 3
Initial Role Contained      : 1
User Dot1x Role Contained   : 5
Dot1x Server Rule           : 5

VLAN Derivation History
=====
VLAN Derivation History Index : 8
1. VLAN 1    for Default VLAN
2. VLAN 1    for Current VLAN updated
3. VLAN 0    for Reset VLANs for Station up
4. VLAN 3    for Default VLAN
5. VLAN 1    for Initial Role Contained
6. VLAN 5    for Dot1x Server Rule
7. VLAN 5    for User Dot1x Role Contained
8. VLAN 5    for Current VLAN updated

Current VLAN : 5 (Dot1x Server Rule)
```

Command History

Release	Modificationa
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa debug dev-id-cache section

```
show aaa debug dev-id-cache section {mac <macaddr>}
```

Description

This command shows section data from ClearPass Policy Manager NetWatch.

Parameter	Description
mac <macaddr>	Shows section data from specified MAC address.

Example

Access the CLI and use the following command to show section data from MAC address **00:1a:1e:aa:bb:cc**:

```
(host) [mynode] #show aaa debug dev-id-cache section mac 00:1a:1e:aa:bb:cc

Device ID Cache Section: cppm Info
-----
Mac Address   Device Type   OS Version   Device Name   Updated At
-----

```

Related Commands

Command	Description
show airgroup	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa debug pmk bss-table

```
show aaa debug pmk bss-table [bssid <bssid>]
```

Description

This command shows information linking the PMK to the BSS.

Parameter	Description
bssid <bssid>	Shows information linking the PMK to the specified BSSID.

Example

The following example shows the authentication survivability cached data:

```
(host) [mynode] #show aaa debug pmk bss-table

PMK BSS-Table
-----
BSSID  Mac Address
-----

Total entries = 0
```

Related Commands

Command	Description
show aaa cluster gsm macuser-section mac	This command displays gsm mac user section for a particular MAC address.
show aaa debug stm message stats	This command shows the number of messages sent/received from STM.
show aaa debug vlan user	This command displays user VLAN derivation related debug information.
show aaa debug dev-id-cache section	This command shows section data from ClearPass Policy Manager NetWatch.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa debug stm message stats

```
show aaa debug stm message stats
```

Description

This command shows the number of messages sent/received from STM.

Example

Access the CLI and use the following command to show the number of messages sent/received from STM:

```
(host) [mynode] #show aaa debug stm message stats

AUTH<-->STM Messages
-----
Msg Type                               Total Msgs
-----
STM sta down                           0
STM ap location                         0
STM sta create H323                    0
STM ap state resp                      0
STM sta state resp                     0
STM tunnel resp                        0
STM monitor time                       0
STM rap user mesg                      0
STM rap user rad acct                  0
STM rap sos user ageout                0
STM rap user rem                       0
STM rap sta state resp                 0
STM rap bridge sta info                0
STM ap global state total              514
STM ap global state add                 0
STM ap global state del                514
STM ap global state modify              0
STM ap global state del sent to ike    505
STM ap global state del not sent to ike 9
STM ap provision state                 0
STM ap authen status                   0
STM FT auth req                        0
STM FT reassoc req                     0
STM FT ask Rldata                      0
STM FT push R0data                     0
STM FT push neighbor                   0
STM restart mesg                       1
STM rap user agent update              0
STM hotspot mesg                       0
STM unknown mesg                       0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa debug vlan user

```
show aaa debug vlan user [ip <ip addr>|ipv6 <ipv6addr>|mac <macaddr>]
```

Description

Displays user VLAN derivation related debug information.

Parameter	Description
ip <ip addr>	User identification based on IPv4 address.
ipv6 <ipv6addr>	User identification based on IPv6 address.
mac <macaddr>	User identification based on MAC address.

Example

The output of the example below displays the VLAN derivation debug information of a user with IPv4 address.

```
(host) #show aaa debug vlan user ip 192.0.2.1

VLAN types present for this User
=====
Default VLAN                : 3
Initial Role Contained      : 1
User Dot1x Role Contained   : 5
Dot1x Server Rule           : 5

VLAN Derivation History
=====
VLAN Derivation History Index : 8
1. VLAN 1    for Default VLAN
2. VLAN 1    for Current VLAN updated
3. VLAN 0    for Reset VLANs for Station up
4. VLAN 3    for Default VLAN
5. VLAN 1    for Initial Role Contained
6. VLAN 5    for Dot1x Server Rule
7. VLAN 5    for User Dot1x Role Contained
8. VLAN 5    for Current VLAN updated

Current VLAN : 5 (Dot1x Server Rule)
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa derivation-rules

```
show aaa derivation-rules [server-group <group-name>|user <name>]
```

Description

Show derivation rules based on user information or configured for server groups.

Parameter	Description
<group-name>	Name of a server group
<name>	Name of a user rule group

Example

The output of the following command shows that the server group group1 has the internal database configured as its authentication server, and that there is a single rule assigned to that group. You can omit the <group-name> parameter to show a table of all your server groups.

```
(host) #show aaa derivation-rules server-group group1

Server Group

Name          Inservice  trim-FQDN  match-FQDN
----          -
Internal      Yes        No

Server Rule Table
-----
Priority  Attribute  Operation  Operand  Action  Value  Total Hits  New
Hits
-----  -
1        Filter-Id  equals     nsFilter  set vlan  111    24
                                0

Rule Entries: 1
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the authentication server assigned to this server group
Inservice	Specifies if the server is in service or out-of-service.

Parameter	Description
trim-FDQN	If enabled, user information in an authentication request is edited before the request is sent to the server.
match-FDQN	If enabled, the authentication server is associated with a specified domain.
Priority	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	This is the attribute returned by the authentication server that is examined for Operation and Operand match
Operation	<p>This is the match method by which the string in Operand is matched with the attribute value returned by the authentication server.</p> <ul style="list-style-type: none"> ■ contains – The rule is applied if and only if the attribute value contains the string in parameter Operand. ■ starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter Operand. ■ ends-with – The rule is applied if and only if the attribute value returned ends with the string in parameter Operand. ■ equals – The rule is applied if and only if the attribute value returned equals the string in parameter Operand. ■ not-equals – The rule is applied if and only if the attribute value returned is not equal to the string in parameter Operand. ■ value-of – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	This is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the rule sets a server group role (set role) or a VLAN (set vlan).
Value	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
Total Hits	Number of times the rule has been applied since the last server reboot.
New Hits	Number of times the rule has been applied since the show aaa derivation-rules command was last issued.

To display derivation rules for a user group, include the `user <name>` parameter. You can also display a table of all user rules by including the `user` parameter, but omitting the `<name>` parameter

```
(host) #show aaa derivation-rules user user44
User Rule Table
-----
Priority  Attribute  Operation  Operand  Action    Value  Total Hits  New
Hits      Description
-----
--
1         location  equals    ap23     18        set role  guest  56
```

The following data columns appear in the output of this command:

Parameter	Description
Priority	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	This is the attribute returned by the authentication server that is examined for Operation and Operand match.
Operation	This is the match method by which the string in Operand is matched with the attribute value returned by the authentication server. <ul style="list-style-type: none"> ■ contains – The rule is applied if and only if the attribute value contains the string in parameter Operand. ■ starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter Operand. ■ ends-with – The rule is applied if and only if the attribute value returned ends with the string in parameter Operand. ■ equals – The rule is applied if and only if the attribute value returned equals the string in parameter Operand. ■ not-equals – The rule is applied if and only if the attribute value returned is not equal to the string in parameter Operand. ■ value-of – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	This is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the rule sets a server group role (set role) or a VLAN (set vlan).

Parameter	Description
Value	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
Total Hits	Number of times the rule has been applied since the last server reboot.
New Hits	Number of times the rule has been applied since the show aaa derivation-rules command was last issued.
Description	This optional parameter describes the rule. If no description was configured then it does not appear when you view the User Table.

Related Commands

Command	Description
aaa derivation-rules	This command configures rules which assigns a AAA profile, user role or VLAN to a client based upon the client's association with an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa device-id-cache

```
show aaa device-id-cache [mac <A:B:C:D:E:F>] [rows number number]
```

Description

This command shows the device ID cache information.

Parameter	Description
mac <A:B:C:D:E:F>	Shows device ID cache information for specified MAC address.
rows number number	Shows device ID cache information for specified rows starting at specified row number.

Example

The following example shows the device ID cache information:

```
(host) [mynode]# show aaa device-id-cache

Device ID Cache
-----
MAC   Device ID   Last Update
---   -
Device ID Cache Entries : 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa dns-query-interval

```
show aaa dns-query-interval <minutes>
```

Description

View the configured interval between DNS requests sent from the controller to the DNS server. If you define a RADIUS server using the FQDN of the server rather than its IP address, the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. By default, DNS requests are sent every 15 minute, but the interval can be changed using the `aaa dns-query-period` command. Issue the `show aaa dns-query-period` command to view the current DNS query interval.

Example

This command shows that the controller will send a DNS query every 30 minutes

```
(host) # show aaa dns-query-period
DNS Query Interval = 30 minutes
```

Related Commands

Command	Description
aaa dns-query-interval	This command configures the DNS query interval.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor and managed devices.

show aaa fqdn-server-names

```
show aaa fqdn-server-names
```

Description

Show a table of IP addresses that have been mapped to fully qualified domain names (FQDNs). If you define a RADIUS server using the FQDN of the server rather than its IP address, the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to view the IP address that currently correlates to each RADIUS server FQDN.

Example

The output of this command shows the IP addresses for two RADIUS servers.

```
(host) #show aaa fqdn-server-names

Auth Server FQDN names
-----
FQDN                IP Address      IPv6 Address    Refcount
----                -
myhost1.example.com 192.0.2.3
2myhost2.example.com 192.0.2.5      3
```

Related Commands

Command	Description
aaa authentication-server radius	This command configures a RADIUS authentication server using that server's fully qualified domain name.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor and managed devices.

show aaa load-balance statistics

show aaa load-balance statistics server-group <sg_name>

Description

Displays the load balancing statistics for RADIUS servers.

Parameter	Description
<sg_name>	Name of the server group.

Example

```
(host) #show aaa load-balance statistics server-group dot1x-test-apsim
Statistics for Radius Servers in Server Group
-----
Server          Acct Rq  Raw Rq  PAP Rq  CHAP Rq  MSCHAP Rq  MSCHAPv2 Rq
Mismatch Rsp  Bad Auth  Acc  Rej  Acct Rsp  Chal  Ukn Rsp  Tmout  Tot Rq
Tot Rsp  Rd Err  Outstanding Auths
-----
-----
abc _RADIUS    0      0      0      0      0      0      26      0
              0      26     0     0      0      0      0      26     26
0              0
AUTOMATIONRAD 0      0      0      0      0      0      207     0
              0      207    0     0      0      0      0      207    207
0              0
```

The output of this command includes the following parameters:

Parameter	Description
Server	Name of the RADIUS server.
Acct Rq	Accounting requests. This reports the number of accounting messages (for example, start/stop/interim update) sent by the controller to a RADIUS server. This counter increments whenever the controller sends one of these messages.
Raw Rq	Raw requests. Number of raw authentication requests the controller sent to a RADIUS server.
PAP Rq	PAP Requests. Number of PAP authentication requests the controller sent to a RADIUS server.

Parameter	Description
CHAP Rq	CHAP requests. Number of CHAP authentication requests the controller sent to a RADIUS server.
MSCHAP Rq	MSCHAP requests. Number of MS-CHAP authentication requests the controller sent to a RADIUS server.
MSCHAPv2 Rq	MSCHAPv2 requests. Number of MS-CHAPv2 requests the controller sent to a RADIUS server.
Mismatch Rsp	Mismatch responses. Number of responses from a RADIUS server for which the controller does not have the proper request context.
Bad Auth	Bad authenticator. Number of responses from the RADIUS server with an invalid secret or bad reply digest.
Acc	Access accept. Number of responses from the RADIUS server with invalid secret or bad reply digest.
Rej	Access reject. Number of responses from the RADIUS server that indicate that client authentication failed.
Acct Rsp	Accounting response. Number of responses sent from the RADIUS server in response to accounting requests sent from the controller.
Chal	Access challenge. Number of responses from the RADIUS server containing a challenge for the client (to complete authentication).
Ukn Rsp	Unknown Response code. Number of responses from the RADIUS server that were not understood by the controller due to the purpose or type of the response
Tmout	Timeouts. Number of messages sent by the controller for which the controller did not receive a response before the message timed out. NOTE: Timeouts include RADIUS accounting requests. Every request controller sends to the RADIUS server is monitored for a timeout, so each retry increments this counter.
AvgRspTme	Average response time. Time taken, on an average, for the RADIUS server to respond to a message from the controller.
Tot Rq	Total errors. This counter reflects the total number of requests sent to the RADIUS server (auth and accounting requests).
Tot Rsp	This counter reflects the total number of responses received by the RADIUS server (auth and accounting responses).

Parameter	Description
Rd Err	Read errors. This counter reflects the total number of errors encountered while reading off socket corresponding to that RADIUS server.
Uptime	Amount of for which the RADIUS server has been active/up. The RADIUS server is considered to have an UP status if the server is active and serving requests. The RADIUS server is considered to be DOWN if the server is not responding. For example, if the RADIUS server does not respond for (<no of retries> * < timeout>) seconds, the controller takes the RADIUS server down. It brings the radius server back into service after the dead timeout.
SEQ	Information corresponding to the sequence number of requests. SEQ total corresponds to the total number of sequence numbers that can be used to communicate with the RADIUS server. SEQ free corresponds to the free/available/not in use sequence numbers for a particular RADIUS server.
Outstanding Auths	This value keeps track of the number of clients that are currently getting authenticated against this authentication server, i.e. clients for which the controller has sent Access-Request but has not yet received Access-Accept or Access-Reject and also the Access-Request has not timed out completely.

Related Commands

Command	Description
aaa authentication-server radius	This command configures a RADIUS authentication server using that server's fully qualified domain name.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa main-profile

show aaa main-profile summary

Description

Displays a summary of all AAA profiles.

Example

The output of the `show aaa main-profile summary` command shows roles, server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show aaa main-profile summary

AAA Profile summary
-----
Name          role      mac-auth  dot1x-  rad-  XML-api  RFC3576  UDR-  ww-  enforce
devtype -dhcp
-----
aaa_dot1x    logon    macprof2  dot1x   RADIUS 10.3.1.15 10.3.15.2  Usr1  Disable
enabled     disabled
default     logon    macprof2  dot1x   RADIUS 10.3.1.15 10.3.15.2  Usr1  Disable
enabled     disabled
default     guest    macprof1  default RADIUS 10.3.1.15 10.3.15.2  Usr2  Disable
enabled     disabled
guest
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the AAA profile.
role	Role for unauthenticated users.
mac-auth	Name of the server group used for MAC authentication.
dot1x-auth	Name of the server group used for dot1x authentication.
rad-act	Name of the server group used for RADIUS authentication.
XML-api	IP address of a configured XML API server.

Parameter	Description
RFC3576	IP address of a RADIUS server that can send user disconnect, session timeout and change-of-authorization messages, as described in RFC 3576.
UDR-group	Name of the user derivation rule profile.
ww-roam	Shows if wired-to-wireless roaming is enabled or disabled.
devtype	Shows if the device identification feature is enabled or disabled. When devtype-classification parameter is enabled, the output of the show user and show user-table commands shows each client's device type, if that client device can be identified.
enforce-dhcp	When this option is enabled, clients must complete a DHCP exchange to obtain an IP address. Best practices are to enable this option when you use the <code>aaa derivation-rules</code> command to create a rule with the DHCP-Option rule type. This parameter is disabled by default.

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor

show aaa multiple-server-accounting statistics server-group

show aaa multiple-server-accounting statistics server-group <sg_name>

Description

This command shows the multiple server accounting statistics for a server-group.

Parameter	Description
<sg_name>	Shows the multiple server accounting statistics for the specified server-group.

Example

The following example shows the multiple server accounting statistics for a server-group corp1:

```
(host) [mynode] #show aaa multiple-server-accounting statistics server-group corp1

Multiple Server Accounting Statistics for Radius Servers in Server Group
-----
Server  Acct Start Req  Acct Interim Req  Acct Stop Req
-----

Acct Start Resp  Acct Interim Resp  Acct Stop Resp  Unknown Resp
-----
```

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Conductor

show aaa password-policy mgmt

show aaa password-policy mgmt [statistics]

Description

Displays the current password policy for management users.

Parameter	Description
statistics	Include this optional parameter to show the numbers of failed login attempts and any lockout periods for management user accounts.

Examples

The output of the `show aaa password-policy mgmt` command below shows that the current password policy requires a management user to have a password with a minimum of 9 characters, including one numeric character and one special character

```
(host) #show aaa password-policy mgmt

Mgmt Password Policy
-----
Parameter Value
-----
Enable password policy          Yes
Minimum password length required      9
Minimum number of Upper Case characters    0
Minimum number of Lower Case characters    0
Minimum number of Digits              1
Minimum number of Special characters (!, @, #, $, %, ^, &, *, <, >, {, }, [, ], :, ., comma, |, +, ~, `) 1
Username or Reverse of username NOT in Password    No
Maximum Number of failed attempts in 3 minute window to lockout user    0
Time duration to lockout the user upon crossing the "lock-out" threshold    3
Maximum consecutive character repeats    0
```

The following data columns appear in the output of this command:

Parameter	Description
Enable password policy	Shows if the defined policy has been enabled

Parameter	Description
Minimum password length required	Minimum number of characters required for a management user password. The default setting is 6 characters.
Minimum number of Upper Case characters	The maximum number of uppercase letters required for a management user password. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.
Minimum number of Lower Case characters	The maximum number of lowercase letters required for a management user password. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.

Parameter	Description
Minimum number of Digits	Minimum number of numeric digits required in a management user password. By default, there is no requirement for digits in a password, and the parameter has a default value of 0.
Minimum number of Special characters	Minimum number of special characters required in a management user password. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0.
Username or Reverse of username NOT in Password	If Yes , a management user's password cannot be the user's username or the username spelled backwards. If No , the password can be the username or username spelled backwards.

Parameter	Description
Maximum Number of failed attempts in 3 minute window to lockout user	Number of times a user can unsuccessfully attempt to log in to the controller before that user gets locked out for the time period specified by the lock-out threshold below. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
Time duration to lockout the user upon crossing the "lock-out" threshold	Amount of time a management user will be "locked out" and prevented from logging into the controller after exceeding the maximum number of failed attempts setting show above. The default lockout time is 3 minutes.
Maximum consecutive character repeats	The maximum number of consecutive repeating characters allowed in a management user password.

Parameter	Description
	By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.

```
(host) #show aaa password-policy mgmt statistics

Management User Table
-----
USER      ROLE    FAILED_ATTEMPTS  STATUS
-----
admin14  root    1                Locked until 12/1/2009 22:28
```

Include the optional `statistics` parameter to show failed login statistics in the Management User table. The example below shows that a single failed login attempt locked out the root user **admin14**, and displays the time when that user can attempt to login to the controller again.

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.
aaa password-policy mgmt	This command define a policy for creating management user passwords.
show references aaa password-policy	This command shows the password policy for locally configured management users.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

show aaa profile

```
show aaa profile <profile-name>
```

Description

Displays configuration details for an individual AAA profile.

Example

The output of the following command shows roles, servers and server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show aaa profile default

AAA Profile "default"
-----
Parameter                                     Value
-----
Initial role                                   logon
MAC Authentication Profile                     N/A
MAC Authentication Default Role               guest
MAC Authentication Server Group               default
802.1X Authentication Profile                 N/A
802.1X Authentication Default Role           guest
802.1X Authentication Server Group           N/A
Download Role from CPPM                       Disabled
Set username from dhcp option 12              Disabled
L2 Authentication Fail Through                Disabled
Multiple Server Accounting                    Disabled
User idle timeout                             N/A
Max IPv4 for wireless user                    2
RADIUS Accounting Server Group                N/A
RADIUS Roaming Accounting                     Disabled
RADIUS Interim Accounting                     Disabled
RADIUS Acct-Session-Id In Access-Request      Disabled
XML API server                                N/A
RFC 3576 server                               N/A
User derivation rules                          N/A
Wired to Wireless Roaming                     Enabled
Reauthenticate wired user on VLAN change      Disabled
Device Type Classification                     Enabled
Enforce DHCP                                  Disabled
PAN Firewall Integration                      Disabled
Open SSID radius accounting                   Disabled
Apply ageout mechanism on bridge mode wireless clients Disabled
Diffie-Hellman Groups Supported for EnhancedOpen 19
```

The following data columns appear in the output of this command:

Parameter	Description
Name	The name of the AAA profile.
Initial Role	Role for unauthenticated users.
MAC Authentication Profile	Name of the MAC authentication profile.
MAC Authentication Default Role	Configured role assigned to the user after MAC authentication.
MAC Authentication Server Group	Name of the server group used for MAC authentication.
8021.X Authentication Profile	Name of the 802.1X authentication profile.
8021.X Authentication Default Role	Configured role assigned to the user after 802.1X authentication.
8021.X Authentication Server Group	Name of the server group used for 802.1X authentication.
Download Role from CPPM	Status of role download from ClearPass Policy Manager. If enabled, the controller downloads the role from ClearPass Policy Manager if not defined.
Set username from dhcp option 12	If enabled, username is set from dhcp option 12 for non-802.1x users.
L2 Authentication Fail Through	To select the other authentication method if one fails.
Multiple Server Accounting	Status of multiple server accounting. If enabled, the controller sends RADIUS accounting to all servers in RADIUS accounting server group.
User idle timeout	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds.
Max IPv4 for wireless user	Maximum number of IPv4 addresses allowed for wireless user.
RADIUS Accounting Server Group	Name of the server group used for RADIUS authentication.

Parameter	Description
RADIUS Roaming Accounting	Displays if Roaming RADIUS accounting service is enabled / disabled, assists in tracking a client who roams to a different AP.
RADIUS Interim Accounting	By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. If RADIUS Interim Accounting is enabled, the controller can also send Interim-Update messages with current user statistics to the server at regular intervals.
RADIUS Acct-Session-Id In Access-Request	When enabled, Acct-Session-Id is included in RADIUS access-request.
XML API server	IP address of a configured XML API server.
RFC 3576 server	IP address of a RADIUS server that can send user disconnect, session timeout and change-of-authorization messages, as described in RFC 3576.
User derivation rules	User attribute profile from which the user role or VLAN is derived.
Wired to Wireless Roaming	Shows whether Wired to Wireless Roaming is Enabled or Disabled .
Reauthenticate wired user on VLAN change	When enabled, wired user is reauthenticated when changing VLANs.
SIP authentication role	For controllers with an installed PEFNG license, this parameter displays the configured role assigned to a session initiation protocol (SIP) client upon registration.
Device Type Classification	Shows if the device identification feature is enabled or disabled. When devtype-classification parameter is enabled, the output of the show user and show user-table commands shows each client's device type, if that client device can be identified.

Parameter	Description
Enforce DHCP	When this option is enabled, clients must complete a DHCP exchange to obtain an IP address. Best practices are to enable this option when you use the <code>aaa derivation-rules</code> command to create a rule with the DHCP-Option rule type. This parameter is disabled by default.
PAN firewall Integration	Displays the status of the PAN firewall integration.
Open SSID Radius Accounting	Displays the Open system SSID RADIUS accounting status.
Apply ageout mechanism on bridge mode wireless clients	Displays the status of ageout mechanism. When enabled, ageout mechanism is applied on bridge mode wireless clients.
Diffie-Hellman Groups Supported for EnhancedOpen	Value set for supported Diffie-Hellman groups for EnhancedOpen. The possible values are 19,20, or 21.

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>RADIUS Roaming Accounting</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

show aaa pubcookie-authentication

```
show aaa pubcookie-authentication
```

Description

This command shows pubcookie authentication configuration.

Example

The following example shows the pubcookie authentication configuration:

```
(host) [mynode] #show aaa pubcookie-authentication
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa radius-attributes

```
show aaa radius-attributes
```

Description

Displays RADIUS attributes recognized by the controller.

Example

The output of the following command shows the name, currently configured value, type, vendor and RADIUS ID for each attribute.

```
(host) #show aaa radius-attributes

Dictionary
-----
Attribute                Value  Type      Vendor      Id
-----                -
MS-CHAP-NT-Enc-PW        6      String    Microsoft   311
Suffix                   1004   String
Menu                     1001   String
Acct-Session-Time        46     Integer
Framed-AppleTalk-Zone    39     String
Connect-Info             77     String
Acct-Ouput-Packets       48     Integer
Aruba-Location-Id        6      String    Aruba        14823
Service-Type              6      Integer
Rad-Length                310    Integer
CHAP-Password             3      String
Aruba-Template-User       8      String    Aruba        14823
Event-Timestamp           55     Date
Login-Service             15     Integer
Exec-Program-Wait        1039   String
Tunnel-Password           69     String
Framed-IP-Netmask         9      IP Addr
Acct-Output-Gigawords     53     Integer
MS-CHAP-CPW-2            4      String    Microsoft   311
Acct-Tunnel-Packets-Lost  86     Integer
Aruba-Captive-Portal-URL  43     String    Aruba        14823
...
```

Related Commands

Command	Description
aaa radius-attributes	This command configures RADIUS attributes to statically configure values to be included in RADIUS Access-Requests and Accounting-Requests.
show references aaa radius-attributes	This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the <code>show aaa radius attributes</code> command is modified to display Aruba-Captive-Portal-URL VSA attribute.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor

show aaa radius modifier

```
show aaa radius modifier <rad_modifier_name>
```

Description

This command displays all the RADIUS modifier profiles.

Example

```
(host) [md] #show aaa radius modifier
Radius Modifier Profile List
-----
Name      References  Profile Status
-----
test      0
test1     0
Total:2
```

Related Commands

Command	Description
aaa radius modifier	This command configures the RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server.
show references aaa radius	This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Command History

Version	Modification
ArubaOS 8.2.0.0	The <code>rad_modifier_name</code> parameter was added.
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor and managed devices.

show aaa rfc-3576-server

```
show aaa rfc-3576-server
<server-ip>
statistics
udp-port
```

Description

Show configuration details for an RFC-3576 server, which is a RADIUS server that can send user disconnect, session timeout and change-of-authorization (CoA) messages, as described in RFC 3576.

Parameter	Description
<server-ip>	IP address of an RFC-3576 server.
statistics	View detailed connection and authentication information for all RFC 3575 servers.
udp-port	Show the configured RFC3576 server port. The default value is port 3799.

Example

This first example shows that there are two configured servers in the RFC 3567 Server List. The **References** column lists the number of other profiles with references to the RFC 3567 server, and the **Profile Status** column indicates whether the server is predefined. User-defined servers will not have an entry in the **Profile Status** column.

```
(host)#show aaa rfc-3567-server

RFC 3576 Server List
-----
Name           References  Profile Status
-----
10.2.14.6      2
```

To view details for a specific server, include the IP address of that server in the command.

```
(host) #show aaa rfc-3576-server 192.0.2.31
RFC 3576 Server "192.0.2.31"
-----
Parameter      Value
-----
Key             *****
```

To view information for all RFC 3576 servers, include the `statistics` parameter.

```
(host)#show aaa rfc-3576-server statistics

RADIUS RFC 3576 Statistics
-----
Statistics          10.1.2.3  10.1.2.34
-----
Disconnect Requests  13         3
Disconnect Accepts   12         3
Disconnect Rejects   1          0
No Secret            0          0
No Session ID        0          0
Bad Authenticator    0          0
Invalid Request      0          0
Packets Dropped      0          2
Unknown service      0          0
CoA Requests         1          0
CoA Accepts          1          0
CoA Rejects          0          0
No permission        0          0

Packets received from unknown clients: 0
Packets received with unknown request: 0
Total RFC3576 packets Received       : 0
```

The output of the `show aaa rfc-3576-server statistics` command includes the following parameters:

Parameter	Description
Disconnect Requests	Number of disconnect requests sent by the server.
Disconnect Accepts	Number of disconnect requests sent by the server that were accepted by the user.
Disconnect Rejects	Number of disconnect requests sent by the server that were rejected by the user.
No Secret	Number of authentication requests that did not contain a RADIUS secret.
No Session ID	Number of authentication requests that did not contain a session ID.
Bad Authenticator	Number of authentication requests that contained a missing or invalid authenticator field in the packet.
Invalid Request	Number of invalid requests.
Packets Dropped	Number of packets dropped.

Parameter	Description
Unknown service	Number of requests for an unknown service type.
CoA Requests	Number of requests for a Change of Authorization (CoA).
CoA Accepts	Number of times a CoA request was accepted.
CoA Rejects	Number of times a CoA request was rejected.
No permission	Number of requests for a service that has been defined, but has not been administratively enabled.

Related Commands

Command	Description
aaa rfc-3576-server	This command define RFC 3576 server profiles.
show references aaa rfc-3576-server	This command shows information about the configuration profiles that reference a specific RFC 3576 server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa server-group

```
show aaa server-group [<group-name>|summary]
```

Description

Displays configuration details for your AAA server groups. Issue this command without the **<group-name>** or **summary** options to display the entire server group list, including profile status and the number of references to each profile. The **References** column lists the number of other profiles that reference a server group, and the **Profile Status** column indicates whether the server group is predefined. User-defined server groups will not have an entry in the Profile Status column.

Parameter	Description
<group-name>	The name of an existing AAA server group.

Examples

This first example shows that there are five configured server groups

```
(host) #show aaa server-group

Server Group List
-----
Name                References  Profile Status
-----
auth-profile-2      1
coltrane-server-group 1
default             25
group1              0
internal            0          Predefined

Total:5
```

To view additional statistics for all server groups, include the `summary` parameter.

```
(host) #show aaa server-group summary

Server Groups
-----
Name                Servers  Rules  hits  Out-of-service
-----
auth-profile-2      1        0     0
coltrane-server-group 1        0     0
default             1        0     0
group1              1        1     0
internal            1        1     0
```

The output of the `show aaa server-group summary` command includes the following parameters:

Parameter	Description
name	Name of an existing AAA server group.
Servers	Number of servers in the group.
Rules	Number of rules configured for the server group.
hits	Number of hits for the server's rules.
Out-of-Service	Indicates whether the server is active, or out of service. Active servers may not have an entry in the Out-of-Service column.

To display detailed authorization, role and vlan statistics for an individual server group, include the name of the group for which you want more information.

```
(host) #show aaa server-group summary group1

Fail Through:No

Auth Servers
-----
Name          Server-Type  trim-FQDN  Match-Type  Match-Op  Match-Str
-----
rad1          Radius      No
company_eng
rad3          Radius      No
company_qa

Role/VLAN derivation rules
-----
Priority  Attribute  Operation  Operand  Action  Value
-----
1         class     contains  admin   set role  root
```

The output of the `show aaa server-group <group-name>` command includes the following parameters:

Parameter	Description
Name	Specifies if the server is in service or out-of-service.
Server-Type	If enabled, user information in an authentication request is edited before the request is sent to the server.
trim-FQDN	If enabled, user information in an authentication request is edited before the request is sent to the server.

Parameter	Description
Match-Type	<p>If the match type is authstring the authentication server associates with a match rule that the controller can compare with the user/client information in the authentication request. A fdqn match type associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request.</p>
Match-Op	<p>This is the match method by which the string in Match-Str is matched with the attribute value returned by the authentication server.</p> <ul style="list-style-type: none"> ■ contains – The rule is applied if and only if the attribute value contains the string in parameter Operand. ■ starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter Operand. ■ ends-with – The rule is applied if and only if the attribute value returned ends with the string in parameter Operand. ■ equals – The rule is applied if and only if the attribute value returned equals the string in parameter Operand. ■ not-equals – The rule is applied if and only if the attribute value returned is not equal to the string in parameter Operand. ■ value-of – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied
Match-Str	<p>This is the string to which the value of the returned attribute is matched.</p>
Priority	<p>The priority in which role or VLAN derivation rules are applied. Rules at the top of the list are applied before rules at the bottom.</p>
Attribute	<p>For role or VLAN derivation rules, this is the attribute returned by the authentication server that is examined for Operation and Operand match.</p>
Operation	<p>For role or VLAN derivation rules, this is the match method by which the string in Operand is matched with the attribute value returned by the authentication server.</p> <ul style="list-style-type: none"> ■ contains – The rule is applied if and only if the attribute value contains the string in parameter Operand. ■ starts-with – The rule is applied if and only if the attribute value returned starts with the string in parameter Operand. ■ ends-with – The rule is applied if and only if the

Parameter	Description
	<p>attribute value returned ends with the string in parameter Operand.</p> <ul style="list-style-type: none"> ■ equals – The rule is applied if and only if the attribute value returned equals the string in parameter Operand. ■ not-equals – The rule is applied if and only if the attribute value returned is not equal to the string in parameter Operand. ■ value-of – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	For role or VLAN derivation rules, this is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the derivation rule sets a server group role (set role) or a VLAN (set vlan).
Value	Sets the user role or VLAN ID to be assigned to the client if the rule condition is met.

Related Commands

Command	Description
aaa server-group	This command allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.
show references aaa server-group	This command shows references to a server group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state ap-group

```
show aaa state ap-group
```

Description

Displays the names and ID numbers of your AP groups

Example

This first example shows that the selected controller has two defined AP groups.

```
(host) #show aaa state ap-group

AP Group Table
-----
Name  ID
----  --
ap1   1
ap2   2
```

Related Commands

Command	Description
ap-group	This command configures an AP group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state configuration

show aaa state configuration

Description

Displays authentication state configuration information, including the numbers of successful and failed authentications.

Example

This example shows authentication settings and values for a controller with no current users.

```
(host) #show aaa state configuration

Authentication State
-----
Name                               Value
----                               -
Switch IP                           10.6.2.253
Switch IPv6
Master/Conductor IP                  10.100.103.253
Switch Role                          local
Current/Max/Total IPv4 Users         0/6/14
Current/Max/Total IPv6 Users         0/1/1
Current/Max/Total User Entries       0/4/15
Current/Max/Total Stations           121/190/367550
Captive Portal Users                 4
802.1X Users                         119
VPN Users                            0
MAC Users                            0
Stateful 802.1X Users                0
Tunneled users                       0
Configured user roles                21
Configured session ACL               41
Configured destinations              32
Configured services                   77
Configured Auth servers              9
Auth server in service                9
Radius server timeouts               7062

Successful authentications
-----
Web  MAC  VPN  802.1X  Krb  RadAcct  SecureID  Stateful-802.1X  Management
---  ---  ---  ---      ---  ---      ---      ---              ---
138  0    0    10117   0    0        0         0                0

Failed authentications
-----
Web  MAC  VPN  802.1X  Krb  RadAcct  SecureID  Stateful-802.1X  Management
---  ---  ---  ---      ---  ---      ---      ---              ---
48   0    0    32235   0    0        0         0                0
```

```

Idled users           = 3366
Mobility              = Enabled
fast age             = Disabled
per-user log         = Disabled
Bandwidth contracts  = 2/1
IP takeovers         = 21
Ping/SYN/Session attacks = 0/0/0

```

The output of the `show aaa state configuration` command includes the following parameters:

Parameter	Description
Switch IP	IP address of the managed device.
Master/Conductor IP	IP address of Mobility Conductor.
Switch Role	Role assigned to the device.
Current/Max/Total IPv4 Users	Current number of IPv4 users on the managed device/Maximum number of IPv4 users that can be assigned to the managed device at any time/Total number of IPv4 users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total IPv6 Users	Current number of IPv6 users on the managed device/Maximum number of IPv6 users that can be assigned to the managed device at any time/Total number of IPv6 users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total Users	Current number of users on the managed device/Maximum number of users that can be assigned to the managed device at any time/Total number of users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total Stations	Current number of stations registered with the controller/Maximum number of stations that can be registered with the controller at any time/Total number of stations that have registered the controller since the last controller reboot.
Captive Portal Users	Number of current users authenticated via captive portal.
802.1X Users	Number of current users authenticated via 802.1X authentication.
VPN Users	Number of current users authenticated via VPN authentication.
MAC Users	Number of current users authenticated via MAC authentication.

Parameter	Description
Stateful 802.1X Users	Number of current users authenticated via stateful 802.1X authentication.
Tunneled users	Number of stations in tunneled forwarding mode, where 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE).
Configured user roles	Number of configured user roles.
Configured session ACL	Number of configured session ACLs.
Configured destinations	Number of destinations configured using the netdestination command.
Configured services	Number of service aliases configured using the netservice command.
Configured Auth servers	Number of configured authentication servers.
Auth server in service	Number of authentication servers currently in service.
Radius server timeouts	Number of times the RADIUS server did not respond to the authentication request.
Web	Total number of captive portal authentications or authentication failures since the last managed device reset.
MAC	Total number of MAC authentications or authentication failures since the last managed device reset.
VPN	Total number of VPN authentications or authentication failures since the last managed device reset.
802.1X	Total number of 802.1X authentications or authentication failures since the last managed device reset.
Krb	Total number of Kerberos authentications or authentication failures since the last managed device reset.
RadAcct	Total number of RADIUS accounting verifications or accounting failures since the last managed device reset.
SecureID	Number of authentication verifications or failures using methods which use one-time passwords. (For example, EAP-GTC being used as the inner EAP protocol of EAP-PEAP.)
Stateful-802.1X	Total number of Stateful 802.1X authentications or authentication failures since the last managed device reset.
Management	Total number of Management user authentications or authentication failures since the last managed device reset.

Parameter	Description
Idled users	Total number of users that are not broadcasting data to an AP.
Mobility	Shows whether the IP mobility feature has been enabled or disabled on the managed device.
Fast age	This parameter shows if fast aging of user table entries has been enabled or disabled. When this feature is enabled, if a device comes up on the network with a different IP address, the device's old IP address is immediately deleted. If the user fast-age feature is not configured, the controller retains up to two IPv4 and two IPv6 addresses per device, and these IPs are aged out only when the device becomes inactive.
Per-User Log	Shows if the managed device collects per-user log files for debugging. NOTE: This option is enabled using the aaa log command.
Bandwidth contracts	Number of configured bandwidth contracts on the managed device.
IP takeovers	Number of times a two different stations have attempted to use the same IP address (IP spoofing).
Ping/SYN/Session attacks	Number of reported ping, SYN and session attacks.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state debug-statistics

```
show aaa state debug statistics
```

Description

Displays debug statistics for controller authentication, authorization and accounting.

Example

The following example displays debug statistics for a variety of authentication errors:

```
(host) #show aaa state debug-statistics
user miss: ARP=47, 8021Q=5216, non-IP=0, zero-IP=0, loopback=0
user miss: mac mismatch=0, spoof=269 (74), drop=390, ncfg=0
user miss: non-auth opcode=0, no-l2-user=0, l2tp=0, vrrp=0, special mac=0,
iap 13 user=0
Idled users = 3376
Idled users due to MAC mismatch = 0
Idled users due to SOS: wireless tunnel=0 wireless dtunnel=0
Idled users due to SOS: wired tunnel=0 wired dtunnel=0
Idled users due to SOS: other=0
Idled users due STM deauth: tunnel=0 dtunnel=0
Idled users from STM timeout: tunnel=0 dtunnel=0
Idled users from STM: other=0
Current users with STM idle flag = 0
Idle messages: SOS=0 STM deauth=0 STM timeout=0
Logon lifetime iterations = 4501, entries deleted = 121
SIP authentication messages received 29227, dropped 29227
Missing auth user deletes: 0
Captive-portal forced user deletes: 1
Mobility Stats
    INTRA_MS 0, MAC mismatch 0, HA mismatch 0
    INTER_MS 0, MAC mismatch 0, HA mismatch 0
    MIP Update 0, Move 0, Del 0, TunAcl 0
    AAA Done 0, Del 2
    IPIP Loop forced Del: 0, Validate Visitor 0
Auth User rejects Received
L2 User:0, IPV4 :0, IPV6:0
Auth User rejects Processed
L2 User:0, IPV4 :0, IPV6:0
```

The **show aaa state debug-statistics** command also displays the number of VIA VPN sessions initiated beyond the assigned limit:

```
(host) [mynode] #show aaa state debug-statistics | include VIA
VIA max session limit exceeded errors: 2
```

The output of this command includes the following parameters:

Parameter	Description
User Miss	
ARP	Number of ARP packets sent between the datapath and the controlpath.
8021q	Number of 802.1q (VLAN tag) packets sent between the datapath and the controlpath.
non-ip	Number of non-IP type packets sent between the datapath and the controlpath.
zero-ip	Number of packets sent without an internet protocol (IP).
loopback	If 1 , the controller has a defined loopback address. If 0 , a loopback address has not yet been configured.
mac mismatch	Number of users that were not authenticated due to MAC mismatches.
spoof	Number of users that were not authenticated due to spoofed IP addresses.
drop	Number of user authentication attempts that were dropped.
ncfg	Number of packets sent between datapath and controlpath, where the authentication module has not completed the initialization required to process the traffic.
Non-auth opcode	Number of packets whose opcode is non-auth opcode. This is a check to find if auth is responsible for processing received packet.
No-l2-user	Number of user packets dropped due to absence of an L2 entry for the user.
l2tp	Number of l2tp users.
vrrp	Number of VRRP users.
special mac	Number of users with a special MAC address.
iap	Number of instant AP users.
idled users	Number of inactive stations that are not broadcasting data to an AP.
idled users due to MAC mismatch	For internal use only.
Idled users due to SOS	

Parameter	Description
wireless tunnel	Number of wireless users in tunnel forwarding mode that were aged out by the controller.
wireless dtunnel	Number of wireless users in decrypt tunnel forwarding mode that were aged out by the controller.
wired tunnel	Number of wired users in tunnel forwarding mode that were aged out by the controller.
wired dtunnel	Number of wired users in decrypt tunnel forwarding mode that were aged out by the controller.
Other	Number of users using modes other than tunneled or Decrypt tunneled aged out by the controller.
Idled users due STM deauth	
tunnel	Number of users in tunnel forwarding mode that aged out after STM deauthentication, and timer expiration.
dtunnel	Number of users in decrypt tunnel forwarding mode that aged out after STM deauthentication, and timer expiration.
Idled users from STM timeout	
tunnel	Number of users in tunnel forwarding mode that aged out after the STM timer expired.
dtunnel	Number of users in decrypt tunnel forwarding mode that aged out after the STM timer expired.
Idled users from STM	
other	Number of users in forwarding modes other than decrypt tunnel or tunnel mode that aged out after the STM timer expired.
Logon lifetime iteration	Number of users deleted for lack of activity.
SIP authentication message	Number of session initiation protocol (SIP) authentication messages received.
Missing auth user deletes	Number of users removed from the datapath by the auth module, even without a mapping entry in control path. This counter can help identify problems with messages sent between the controlpath and the datapath.
Mobility Stats	Number of different messages exchanged between the mobile IP and the auth module. This is used for troubleshooting purposes only.

Parameter	Description
<code>Captive-portal forced user deletes</code>	Number of idle users deleted after captive portal authentication.
Auth User Rejects Received	
<code>L2 User</code>	Number of authentication rejects received for L2 users from the datapath due to a failure of the operation.
<code>IPv4</code>	Number of authentication rejects received for IPv4 users from the datapath due to a failure of the operation.
<code>IPv6</code>	Number of authentication rejects received for IPv6 users from the datapath due to a failure of the operation.
Auth User Rejects Processed	
<code>L2 User</code>	Number of authentication rejects for L2 users that were processed after the reject was received.
<code>IPv4</code>	Number of authentication rejects for IPv4 users that were processed after the reject was received.
<code>IPv6</code>	Number of authentication rejects for IPv6 users that were processed after the reject was received.

Command History

Release	Modification
ArubaOS 8.11.0.0	The show aaa state debug-statistics command displays the number of VIA VPN sessions initiated beyond the assigned limit.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state log

show aaa state log [info]

Description

Displays global log files for AAA events. If you have enabled per-user logging using the [aaa log](#) command, the output of this command displays global AAA log files for events that are not triggered by individual user authentication, such as AP authentication and the initial pre-authentication processes that occur before a client authenticates to the controller.

To display log files for events triggered by a specific user, use the command [show user](#) or `show ipv6 user-table ip <ipv6-addr> log`.

Parameter	Description
info	This parameter displays debugging information for internal use only.

Example

The example below shows a partial list of the global log files displayed by the `show aaa state log` command..

```
(host) #show aaa state log
1: At Thu Apr 11 10:41:27: [L] Type cert-downloaded * id 0 len 0,
  bssid 00:00:00:00:00:00 | mac: 00:00:00:00:00:00
2: At Thu Apr 11 10:43:17: [L] Type ap-up * id 0 len 0,
  bssid 6c:f3:7f:5f:2c:b0 | mac: 00:00:00:00:00:00
3: At Thu Apr 11 10:43:17: [L] Type ap-up * id 0 len 0,
  bssid 6c:f3:7f:5f:2c:a0 | mac: 00:00:00:00:00:00
4: At Thu Apr 11 10:43:50: [L] Type station-term-start * id 10 len 0,
  bssid 6c:f3:7f:5f:2c:a0 | mac: 50:a4:c8:bd:be:41
5: At Thu Apr 11 10:43:50: [L] Type station-data-ready_ack * id 10 len 0,
  bssid 00:00:00:00:00:00 | mac: 50:a4:c8:bd:be:41
```

Related Commands

Parameter	Description
aaa log	Issue this command to enable per-user logging.
show user show ipv6 user-table	Display log files for authentication events triggered by a specific IPV4 or IPV6 user.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

16	ace	5519	5519	0
0				
17	user	781821	781821	0
0				
27	bwm	3	3	0
0				
29	wkey	27109	27109	4
4				
42	nat	1	1	0
0				
43	user tmout	4164	4164	4160
4160				
56	forw unenc	1787103	1787103	0
0				
64	auth	5268	5268	5267
5267				
94	aescm key	17885	17885	0
0				
111	dotlx term	196813	196813	151161
151161				
114	rand	1614	1614	1612
1612				
126	eapkey	1316231	1316231	2632462
2632462				
114	rand	2	2	0
0				

The output of this command contains the following parameters:

Parameter	Description
Msg ID	ID number for the message type.
Name	Message name.
Since last Read	Number of messages received since the buffer was last read.
Total	Total number of message received since the controller was last reset.
opcode	Code number of the message type.
Sent Since last Read	Number of messages sent since the buffer was last read.
Sent Total	Total number of message sent since the controller was last reset.
Recv Since last Read	Number of messages received since the buffer was last read.
Recv Total	Total number of message received since the controller was last reset.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state mux-tunnel

Description

Displays multiplexer (MUX) tunnel IDs.

Example

The example below shows statistics for one MUX tunnel

```
(host) #show aaa state mux-tunnel
Mux Tunnel Information
-----
      IP           Tunnel ID      Slot/Port  AP Type  AP Name
-----
10.2.1.26          1/1                1
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of a multiplexer (MUX) server
Tunnel ID	ID number of a MUX tunnel.
Slot/Port	The slot and port used by the controller, in the format <slot>/<module>/<port>
AP Type	AP model type.
AP Name	Name of an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state station

```
show aaa state station <A:B:C:D:E:F>
```

Description

Displays AAA statistics for a station.

Parameter	Description
<A:B:C:D:E:F>	MAC address of a station.

Example

The example below shows statistics for a station with four associated user IP addresses. The output of this command shows station data, the AAA profiles assigned to the station, and the station's authentication method.

```
(host) #show aaa state station 00:21:5c:85:d0:4b
Association count = 1, User count = 4
User list = 10.1.10.10 10.6.5.168 192.168.229.1 192.168.244.1
ssid: ethersphere-wpa2, bssid: 00:1a:1e:8d:5b:31 AP name/group:
AL40/corp1344 PHY: a, ingress=0x10e8 (tunnel 136)
vlan default: 65, assigned: 0, current: 65 cached: 0, user derived: 0, vlan-
how: 0
name: MYCOMPANY\tgonzales, role:employee (default:logon, cached:employee,
dot1x:), role-how: 1, acl:51/0, age: 00:02:50
Authentication: Yes, status: successful, method: 802.1X, protocol: EAP-MD5,
server: vortex
dot1xctx:1 sap:1
Flags: mba=0
AAA prof: default-corp1344, Auth dot1x prof: default, AAA mac prof:, def
role: logon
ncfg flags udr 1, mac 0, dot1x 1
Born: 1233767066 (Wed Feb  4 09:04:26 2009
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state tunneled-node

show aaa state tunneled-node

Description

This command shows tunnels originating from the tunnel nodes.

Example

The following example shows tunnels originating from the tunnel nodes:

```
(host) [mynode] #show aaa state tunneled-node

Tunnel Information
-----
      IP           Tunnel ID      Port  AP Type  AP Name
-----
-----
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa state user

show aaa state user <A.B.C.D>

Description

Displays statistics for an authenticated user.

Parameter	Description
<A.B.C.D>	IP address of a user.

Example

The example below shows statics for a user with the IP address 10.1.10.11. The output of this command shows user data, the user's authentication method, and statistics for assigned roles, timers and flags.

```
(host) #show aaa state user 10.1.10.11
Name: MYCOMPANY\tsenter, IP: 10.1.10.11, MAC: 00:21:5c:85:d0:4a,
Role:employee, ACL:51/0, Age: 00:01:46
Authentication: Yes, status: successful, method: 802.1X, protocol: EAP-MD5,
server: vortex
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: Default
VLAN Derivation: Matched user rule
Idle timeouts: 0, ICMP requests sent: 0, replies received: 0, Valid ARP: 0
Mobility state: Associated, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0
L3 Mob: 0
Flags: internal=0, trusted_ap=0, delete=0, l3auth=0, l2=1 mba=0
Flags: innerip=0, outerip=0, guest=0, station=0, download=1, nodatapath=0
Auth fails: 0, phy_type: a-HT, reauth: 0, BW Contract: up:0 down:0, user-
how: 1
Vlan default: 65, Assigned: 0, Current: 65 vlan-how: 0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, ProxyArp=0, Flags=0x0
Tunnel=0, SlotPort=0x1018, Port=0x10e2 (tunnel 130)
Role assigned: n/a, VPN: n/a, Dot1x: Name: employee role-how: 0
Essid: ethersphere-wpa2, Bssid: 00:1a:1e:11:6b:91 AP name/group:
AL31/corp1344 Phy-type: a-HT
RadAcct sessionID:n/a
RadAcct Traffic In 0/0 Out 0/0 (0:0/0:0:0:0,0:0/0:0:0:0)
Timers: arp_reply 0, spoof_reply 0, reauth 0
Profiles AAA:default-corp1344, dot1x:default, mac: CP: def-role:'logon' sip-
role:''
ncfg flags udr 0, mac 0, dot1x 0
Born: 1233772328 (Wed Feb 4 10:32:08 2009)
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa state user-tunneled-node

```
show aaa state user-tunneled-node
```

Description

This command shows tunnels originating from the HP switch user tunnels.

Example

The following example shows tunnels originating from the HP switch user tunnels. :

```
(host) [mynode] #show aaa state user-tunneled-node

Per User Tunnel Information
-----
Client MAC      UserName      Auth      Switch IP      Switch Port      GRE Key
Switch Mac      -----
-----
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show aaa tacacs-accounting

show aaa tacacs-accounting

Description

Displays TACACS accounting configuration.

Example

The example below shows that TACACS accounting has been enabled, and that the TACACS server is in the server group acct-server.

```
(host) #show aaa tacacs-accounting
TACACS Accounting Configuration
-----
Parameter  Value
-----  ----
Mode       Enabled
Server-Group acct-server
```

The output of this command includes the following parameters:

Parameter	Description
Mode	Shows if the TACACS accounting feature is enabled or disable
Server-Group	The server group that contains the active TACACS server.

Related Commands

Command	Description
aaa tacacs-accounting	This command configures reporting of commands issued from a managed device to a TACACS+ server group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa timers

```
show aaa timers
```

Description

Displays AAA timer values.

Example

The example below shows that the controller has all default timer values:

```
(host) #show aaa timers
User idle timeout = 6 minutes
Auth Server dead time = 10 minutes
Logon user lifetime = 5 minutes
```

Related Commands

Command	Description
aaa timers	This command configures the timers that you can apply to clients and servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa user-delete-result

```
show aaa user-delete-result
```

Description

This command displays the list of users deleted for the last twenty delete requests issued from the Managed devices. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays the user deleted from the Managed Devices,

```
(host)[mynode] (config) #show aaa user-delete-result
Summary of user delete CLI requests !
Current user delete request timeout value: 300 seconds

aaa user delete 1.2.3.4 , Overall Status- Complete , Total users deleted- 0
MD IP : 10.9.196.168, Status- Complete , Count- 0
MD IP : 10.3.67.30, Status- Complete , Count- 0
```

Related Commands

Command	Description
aaa user delete	This command deletes clients, users, or roles.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa web admin-port

```
show aaa web admin-port
```

Description

Displays the port numbers of HTTP and HTTPS ports used for web administration.

Example

The example below shows that the controller is configured to use HTTPS on port 4343 or 443, and HTTP on port 8888.

```
(host) #show aaa web admin-port
https port = 4343
http port = 8888
```

Command History

Command	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa xml-api server

```
show aaa xml-api server [<server_ip>]
```

Description

Displays a list of XML servers used for authentication, authorization, and accounting.

Parameter	Description
<server_ip>	IP address of an XML API server. Include this parameter to see if a secret key is configured for the specified server.

Example

The output of this command shows that the Mobility Conductor has two configured XML API servers that are each referenced by two different AAA profiles. Note that user-defined servers will not have an entry in the **Profile Status** column.

```
(host) #show aaa xml-api server

XML API Server List
-----
Name    References Profile Status
-----
10.1.2.3 2
10.4.3.2 2
```

Related Commands

Command	Description
aaa xml-api	This command configures an external XML API server.
show references aaa xml-api server	This command shows references to an XML API Server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show aaa xml-api statistics

show aaa xml-api statistics

Description

Displays statistics for an external XML API server. Issue this command to troubleshoot AAA problems and monitor usage on an XML server.

Parameter	Description
<server_ip>	IP address of XML API server.

Example

The example below shows AAA statistics for an external XML server with the IP address 10.1.2.3. This command shows the number of times that a particular event has occurred per client. The first number is the number of times this event occurred. The number of new events since the last time the counters were displayed is shown in parentheses.

```
(host) #show aaa xml-api statistics

ECP Commands Statistics
-----
Server user_authenticate user_add user_delete user_denylist user_query
user_logout
-----
-----
ECP Errors Statistics
-----
Server UnkUser UnkRole UnkExtAgent AuthFail InvCmd InvMsgAuth
InvMsgDig MsgAuthMiss InvVerNo IntErr ClntNotAuthz VlanIP InvIP
SwitchIP MacAddrMiss UnsuppCmd OperTimeout
-----
-----
Packets received from unknown clients : 0 (0)
Packets received with unknown request : 0 (0)
Requests Received/Success/Failed      : 0/0/0 (0/0/0)
```

The output of this command includes the following parameters:

Parameter	Description
user_authenticate	Number of users authenticated on the XML server since the last controller reboot.
user_add	Number of users added to the controller's user table.
user_delete	Number of users removed from the controller's user table.
user_blacklist/user_denylist	Number of denied user association requests.
user_query	Number of user queries performed.
unknown user	Number of unknown users.
unknown role	Number of unknown user roles.
unknown external agent	Number of requests by an unknown external agent.
authentication failed	Number of failed authentication requests.
invalid command	Number of invalid XML commands
invalid message authentication method	Number of XML commands with an invalid authentication method (when a key is configured on the controller).
invalid message digest	Number of XML commands with an invalid digest type (when a key is configured on the controller).
missing message authentication	Number of XML commands with an missing authentication method (when a key is configured on the controller).
missing or invalid version number	Number of commands with a missing or invalid version number. The version number should always be 1.0.
internal error	Number of internal server errors
client not authorized	Number of unauthorized clients
Cant use VLAN IP	Number of time a user IP is same as the VLAN IP.
Invalid IP	Number of XML commands with an invalid IP address.
Cant use Switch IP	Redirection to a IP failed, possibly because the source IP has been NATted.

Parameter	Description
missing MAC address	Number of XML commands with a missing MAC address.
Packets received from unknown clients	Number of packets received from unknown clients.
Packets received with unknown request	Number of packets received with unknown request
Requests Received/Success/Failed	Total number of requests received / number of successful requests / number of failed requests

Command History

Command	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show acl ace-table

```
show acl ace-table {ace <0-7680>}|{acl <1-2699>}|{all}
```

Description

Displays an access list entry (ACE) table for an ACL.

Parameter	Description
ace <0-7680>	Shows a single ACE entry.
acl <1-2699>	Shows all ACE entries for a single ACL.
all	Shows all ACE entries.

Example

The following example shows that there are eighteen access control entries for ACL 1.

```
(host) #show acl ace-table acl 1
1020: any any 1 0-65535 0-65535 f80001:permit
1021: any any 17 0-65535 53-53 f80001:permit
1022: any any 17 0-65535 8211-8211 f80001:permit
1023: any any 17 0-65535 8200-8200 f80001:permit
1024: any any 17 0-65535 69-69 f80001:permit
1025: any any 17 0-65535 67-68 f80001:permit
1026: any any 17 0-65535 137-137 f80001:permit
1027: any any 17 0-65535 138-138 f80001:permit
1028: any any 17 0-65535 123-123 f80001:permit
1029: user 10.6.2.253 255.255.255.255 6 0-65535 443-443 f80001:permit
1030: user any 6 0-65535 80-80 d1f90,0000 f80021:permit dnat
1031: user any 6 0-65535 443-443 d1f91,0000 f80021:permit dnat
1032: any any 17 0-65535 500-500 f80001:permit
1033: any any 50 0-65535 0-65535 f80001:permit
1034: any any 17 0-65535 1701-1701 f80001:permit
1035: any any 6 0-65535 1723-1723 f80001:permit
1036: any any 47 0-65535 0-65535 f80001:permit
1037: any any 0 0-0 0-0 f180000:deny
```

Related Commands

Command	Description
ip access-list session	This command configures an ACL session. To create IPv6 specific rules, use the ipv6 keyword.

Command History

Release	Modification
ArubaOS 8.2.0.0	The new range for ace and acl were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show acl acl-table

```
show acl acl-table  
  <1-2699>  
  verbose
```

Description

Displays information for a specified ACL.

Parameter	Description
acl-table <1-2699>	Specify the number of the ACL for which you want to view information.
verbose	Show verbose ACL information.

Example

The following example displays the ACL table for the controller:

```
(host) #show acl acl-table 1  
  
AcLTable  
-----  
ACL  Type  ACE Index  Ace Count  Name  Applied  
---  ---  -----  -  
1    role  1459      18         logon  0  
  
Total free ACE entries = 3591  
Free ACE entries at the bottom = 2552  
Next ACE entry to use = 1480 (table 1)  
Ace entries reused 622 times  
ACL count 64, tunnel acl 0  
  
Ace entries reused 373 times  
ACL count 64, tunnel acl 0
```

The output of this command displays the following parameters:

Parameter	Description
ACL	Number of the specified ACL
Type	Shows the ACL type: <ul style="list-style-type: none">■ role: Access list is used to define a user role.■ mac: MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of

Parameter	Description
	MAC addresses. <ul style="list-style-type: none"> ■ session: Session ACLs define traffic and firewall policies on the controller. ■ ether-type: This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. ■ standard: Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.
ACE Index	Starting index entry for the ACL's access control entries
ACE Count	Number of access control entries in the ACL
Name	Name of the ACL.
Applied	Number of times the ACL was applied to a role.
Total free ACE entries	The total number of free ACE entries. This includes available ACE entries at the bottom of the list, as well as free ACE entries in the middle of the table from previous access list entries that were later removed.
Free ACE entries at the bottom	The total number of free ACE entries at the bottom of the list.
Next ACE entry to use	Ace number of the first free entry at the bottom of the list.
ACE entries reused	For internal use only.
ACL count	Total number of defined ACLs
Tunnel ACL	Total number of defined tunnel ACLs.

The following example displays the ACL table in verbose mode:

```
(host) [mynode] #show acl acl-table verbose
AclTable
-----
ACL  Type          ACE Index  Rule Count  Ace Count  Name
    Applied  Alias-Rule-Hits
---  ---
-----
1    session      0          0           1          global-sacl
    0          Disabled
2    role         535        32          33         logon
    0          Disabled
3    session      241        11          12         validuser
    0          Disabled
```

```

4    session      0      0      1      sdn-acl
    0      Disabled
5    route        6      0      1      uplink-lb-cfg-racl
    0      Disabled

```

```

Total ACE entries in use = 503
Total free ACE entries = 15369
Free ACE entries at the bottom = 15273
Next ACE entry to use = 599 (table 1)
Ace entries reused 1 times
ACL count 93, tunnel acl 0
ACE table toggle count = 2
Total hits table indices in use = 0
Total free hits table indices = 16384
Free hits table indices at the bottom = 16384
Next hits table index entry to use = 0 (table 1, toggle-count 2)

```

The output of this command displays the following parameters:

Parameter	Description
ACL	Number of the specified ACL.
Type	Shows the ACL type: <ul style="list-style-type: none"> ■ role: Access list is used to define a user role. ■ session: Session ACLs define traffic and firewall policies on the controller. ■ route: Name of the route for which you want to record advanced debugging information.
ACE Index	Starting index entry for the ACL's access control entries.
Rule Count	Total rule count of ACLs.
ACE count	Number of access control entries in the ACL.
Name	Name of the ACL.
Applied	Number of times the ACL was applied to a role.
Alias-Rule-Hits	Total number of alias rule hits.
Total Ace entries in use	Total number of ACE entries in the table.
Total free ACE entries	The total number of free ACE entries. This includes available ACE entries at the bottom of the list, as well as free ACE entries in the middle of the table from previous access list entries that were later removed.

Parameter	Description
Free ACE entries at the bottom	The total number of free ACE entries at the bottom of the list.
Next ACE entry to use	ACE number of the first free entry at the bottom of the list.
ACE entries reused	For internal use only.
ACL count	Total number of defined ACLs.
Tunnel ACL	Total number of defined tunnel ACLs.
ACE table toggle count	ACE table toggles between those banks on configuration events, and the toggle count is a counter for that operation.
Total hits table indices in use	Count that represents the hits-table indices used by ACEs with netdestinations.
Total free hits tables indices	The total number of free hits-table entries.
Free hits table indices at the bottom	The total number of free hits-indices at the bottom of the table.
Next hits table index entry to use	Hits-table index of the first free entry at the bottom of the table.

Related Commands

Command	Description
ip access-list session	This command configures ACLs.
show ap debug acl-table	This command shows ACL table in AP datapath.

Command History

Release	Modification
ArubaOS 8.8.0.0	Parameter <code>verbose</code> was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show acl hits

```
show acl hits
```

Description

Displays internal ACL hit counters. Issue this command to see the number of times an ACL defined a user's role, or traffic and firewall policies for a user session.

Example

In the example below, the output of the *User Role ACL Hits* table is shown in two separate tables to allow the output to fit on a single page of this document. In the actual controller CLI, the *User Role ACL Hits* table is shown in a single, wide table.

```
(host) #show acl hits
User Role ACL Hits
-----
Role          Policy          Src          Dst
----          -
logon         control         any          any
logon         control         any          any
logon         control         any          any
visitor      vp-control      any          any
visitor      vp-control      any          any
visitor      vp-access      any          any
visitor      vp-access      user         mswitch-master/
conductor
visitor      vp-access      any          any

Service/      Action   Dest/Opcode  New Hits  Total Hits  Index      Ipv4/Ipv6
Application
-----
svc-icmp      permit   0             0         6           5052      IPv4
svc-dhcp      permit   0             0         2           5057      IPv4
0             deny    0             0         53          5069      IPv4
svc-dns       permit   9             46079    4885        4885      IPv4
svc-dhcp      permit   0             788      4886        4886      IPv4
svc-icmp      permit   0             536      4887        4887      IPv4
svc-http      permit   0             41       4889        4889      IPv4
6 9100-9100   permit   0             31       4892        4892      IPv4

Port Based Session/Route ACL
-----
Policy      Src          Dst  Service  Action  Dest/Opcode  New
Hits Total Hits  Index Ipv4/Ipv6
-----
--
validuser  10.1.1.0 255.255.255.0  any  any    deny         0
214      4655     IPv4
```

```

validuser any          any any      permit          6
 2502          4656      IPv4
Port ACL Hits
-----
ACL      ACE      New Hits      Total Hits      Index      Ipv4/Ipv6
---      ---      -
5        22       0             14             238       IPv4

```

The output of this command includes the following information:

Parameter	Description
Role	Name of the role assigned by the ACL.
Policy	Name of the policy used by the ACL
Src	The traffic source, which can be one of the following: <ul style="list-style-type: none"> ■ <alias>: Name of a user-defined alias for a network host, subnetwork, or range of addresses. ■ any: match any traffic. ■ host: specify a single host IP address. ■ network: specify the IP address and netmask. ■ user: represents the IP address of the user.
Dst	The traffic destination, which can be one of the following: <ul style="list-style-type: none"> ■ <alias>: Name of a user-defined alias for a network host, subnetwork, or range of addresses. ■ any: match any traffic. ■ host: specify a single host IP address. ■ network: specify the IP address and netmask. ■ user: represents the IP address of the user.
Service	Network service, which can be one of the following: <ul style="list-style-type: none"> ■ IP protocol number (0-255) ■ name of a network service (use the show netservice command to see configured services) ■ any: match any traffic ■ tcp: specify the TCP port number (0-65535) ■ udp: specify the UDP port number (0-65535)
Action	Action if rule is applied, which can be one of the following: <ul style="list-style-type: none"> ■ deny: reject packets ■ dst-nat: perform destination NAT on packets ■ dual-nat: perform both source and destination NAT on packets ■ permit: forward packets ■ redirect: specify the location to which packets are redirected ■ src-nat: perform source NAT on packets
Dest/Opcode	The datapath destination ID.

Parameter	Description
New Hits	Number of ACL hits that occurred since this command was last issued.
Total Hits	Total number of ACL hits recorded since the controller last reset.
Index	Index number of the ACL.
ACL	ACL number
ACE	ACE number
New Hits	Number of times the ACL was applied since this command was last issued.
Total Hits	Number of times the ACL was applied since the controller was last reset.
Index	Index number of the ACL.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show activate

show activate

Description

This command displays the profile that allows a managed device to synchronize its remote AP whitelist/allowlist with the Aruba Activate cloud-based services.

Use this command to view the credentials the managed device uses to synchronize the remote AP whitelist/allowlist with an Activate server.

Example

The following example displays the Activate whitelist/allowlist service settings:

```
(host)[node](config)# show activate
activate
-----
Parameter                               Value
Set                                       -----
---
Activate AP Whitelist/Allowlist Service   nabled
Activate Device Whitelist/Allowlist Service nabled
Activate URL                              https://activate.arubanetworks.com
Provision Activate URL                    https://device.arubanetworks.com
Activate Login Username                   ztp
Activate Login Password                   *****
Periodic Interval for WhiteList Download  1
Add-Only Operation                        Enabled
Custom cert to upload to Activate         N/A
Server cert to be used for IPSEC          N/A
```



The **Periodic Interval for WhiteList/Allowlist Download** parameter indicates the whitelist/allowlist download period in days.

Related Commands

Parameter	Description
activate	This command synchronizes the remote AP whitelist/allowlist on the managed device with the Activate whitelist/allowlist database.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following terminologies are updated: <ul style="list-style-type: none">▪ All instances of <code>master</code> have been replaced with <code>conductor</code>.▪ All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or enable mode on Mobility Conductor.

show adp config

```
show adp config
```

Description

Displays Aruba Discovery Protocol (ADP) configuration settings.

Example

The following example shows that the managed device has all default settings for ADP.

```
(host) [mynode] (config) #show adp config
ADP Configuration
-----
key          value
---          -
discovery    enable
igmp-join    enable
igmp-vlan    0
```

The output of this command includes the following parameters:

Parameter	Description
discovery	Aruba APs send out periodic multicast and broadcast queries to locate Mobility Conductor. If the APs are in the same broadcast domain as Mobility Conductor and ADP is enabled on the managed device, the managed device automatically responds to the APs' queries with its IP address. This command shows whether ADP is enabled or disabled on the managed device.
igmp-join	Shows whether the managed device has enabled or disabled the sending of Internet Group Management Protocol (IGMP) join requests.
igmp-vlan	ID of the VLAN to which IGMP reports are sent. If this value is set to 0, the managed device will use the default route VLAN used.

Related Commands

Command	Description
	This command configures the ADP.

Command	Description
adp	

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show adp counters

```
show adp counters
```

Description

Displays Aruba Discovery Protocol (ADP) counters.

Example

The following example shows the ADP counter table for the managed device.

```
(host)[mynode](config) #show adp counters
ADP Counters
-----
key          value
---          -
IGMP Join Tx 1
IGMP Drop Tx 0
ADP Tx       0
ADP Rx       0
```

The output of this command includes the following parameters:

Parameter	Description
IGMP Join Tx	Number of Internet Group Management Protocol (IGMP) join requests sent by the managed device.
IGMP Drop Tx	Number of Internet Group Management Protocol (IGMP) drop requests sent by the managed device.
ADP Tx	Number of ADP responses sent to APs.
ADP Rx	Number of multicast and broadcast queries received from APs trying to locate Mobility Conductor.

Related Commands

Command	Description
adp	This command configures the ADP.
show adp config	Show Aruba Discovery Protocol (ADP) configuration settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup

```
show airgroup
  active-domains
  aps
  blocked-queries [dlna|mdns]
  blocked-service-id [dlna|mdns]
  cache entries [dlna|mdns|static|verbose]
  cppm [entries|server-group]
  cppm-server {aaa|query-interval|{radius statistics}|{rfc3576 statistics}}
  domain
  effective profiles
  flow-table
  internal-state statistics {dlna|mdns|ppm
  {daily|hourly|minutes|weekly|<count>}|verbose}
  multi-controller-table {dlna|mdns|verbose}
  packet-capture {hex|in-pkt|mac|out-pkt|tcpdump-options|write-to-flash|<count>}
  ppm
  policy-entries [mac {neighborhood <macaddr>}|<macaddr>]
  query-result
  servers {dlna|mdns|verbose}
  status
  switches
  tracebuf [msgs [ip <ipaddr>]|[mac <macaddr>]]|pps]
  thread-statistics
  users {dlna|mdns|verbose}
  vlan
```

Description

This command shows the global AirGroup settings. Click parameter links to view the corresponding show commands.

Parameter	Description
active-domains	Shows list of configured AirGroup active-domains. NOTE: This command is not applicable when Mobility Conductor is a VM.
aps	Shows the AP table. NOTE: This command is not node specific.
blocked-queries dlna mdns	Shows dropped query IDs because the associated service is unavailable. <ul style="list-style-type: none">▪ dlna - Shows the blocked DLNA queries.▪ mdns - Shows the blocked mDNS

Parameter	Description
	<p>queries.</p> <p>NOTE: This command is not node specific.</p>
<p><u>blocked-service-id</u></p> <p>dlna mdns</p>	<p>Shows blocked service IDs.</p> <ul style="list-style-type: none"> ▪ dlna - Shows the blocked DLNA service IDs. ▪ mdns - Shows the blocked mDNS service IDs. <p>NOTE: This command is not node specific.</p>
<p><u>cache entries</u></p> <p>dlna mdns static verbose</p>	<p>Shows DLNA and mDNS cache entries.</p> <ul style="list-style-type: none"> ▪ dlna - Shows the DLNA cache entries. ▪ mdns - Shows the mDNS cache entries. ▪ static - Shows the static cache entries. ▪ verbose - Shows additional details of airgroup cache entries <p>NOTE: This command is node specific.</p>
<p><u>cppm</u></p> <p>entries server-group</p>	<p>Shows ClearPass Policy Manager details.</p> <ul style="list-style-type: none"> ▪ entries: Shows information for devices registered in ClearPass Policy Manager. This command is not node specific. ▪ server-group: Shows ClearPass Policy Manager server group information. This command is node specific.
<p><u>cppm-server</u></p> <p>aaa query-interval radius statistics rfc3576 statistics</p>	<p>Shows ClearPass Policy Manager server details.</p> <ul style="list-style-type: none"> ▪ aaa: Shows the AAA parameters for AirGroup. ▪ query-interval: Shows the query interval used to refresh the ClearPass Policy Manager entries at periodic intervals. ▪ radius statistics: Shows the RADIUS statistics. This command is node specific. ▪ rfc3576 statistics: Shows the dynamic authorization extensions to RADIUS statistics. This command is node specific.

Parameter	Description
domain	Shows the IP address of participating managed devices.
effective profiles	Shows the effective profiles that are applied at that node. NOTE: This command is node specific.
flow-table	Shows the flows installed by AirGroup process. NOTE: This command is node specific.
internal-state statistics dlna mdns ppm{daily hourly minutes weekly <count>} verbose	Shows internal state of AirGroup process. <ul style="list-style-type: none"> ▪ dlna - Shows the DLNA statistics. ▪ mdns - Shows the mDNS statistics. ▪ ppm - Shows packet per minute statistics. ▪ verbose - Shows additional details of the statistics. NOTE: This command is not node specific.
multi-controller-table dlna mdns verbose	Show the AirGroup cluster information. <ul style="list-style-type: none"> ▪ dlna - Shows DLNA statistics. ▪ mdns - Shows mDNS statistics, ▪ verbose - Shows additional details of the statistics. NOTE: This command is not applicable when Mobility Conductor is a VM. NOTE: This command is supported only on stand-alone controller domain.
packet-capture	Show packet capture in one of the following formats: <ul style="list-style-type: none"> ▪ hex: Show packet capture in HEX format ▪ in-pkt: Show packet capture received (RX). ▪ mac: Show packet capture filter with MAC address. ▪ out-pkt: Show packet capture sent (TX). ▪ tcpdump-options: Show packet capture

Parameter	Description
	filter tcpdump options. <ul style="list-style-type: none"> ▪ write-to-flash: Save packet capture to ag.pcap. ▪ <count>: Show last count rows.
<u>policy-entries</u> mac neighborhood <mac> <mac>	Show the active policies. <ul style="list-style-type: none"> ▪ neighborhood - Shows the AP neighborhood to discover the server. ▪ mac - Shows active policies filtered by specified MAC address. <p>NOTE: This command is not node specific.</p>
<u>query-result</u>	Shows the list of servers available for the query sent.
<u>servers</u> dlna mdns verbose	Shows the server table. <ul style="list-style-type: none"> ▪ dlna - Shows the DLNA servers. ▪ mdns - Shows the mDNS servers. ▪ verbose - Shows additional information of the AirGroup servers. <p>NOTE: This command is node specific.</p>
<u>status</u>	Shows the current status of the AirGroup configuration and configured AirGroup services. <p>NOTE: This command is node specific.</p>
switches	Shows the switch entries. <p>NOTE: This command is node specific.</p>
<u>tracebuf</u> msgs [ip <ipaddr>][mac <macaddr>] pps	Shows the trace buffer. <ul style="list-style-type: none"> ▪ msgs - Shows the AirGroup trace buffer. ▪ pps - Shows the packet arrival trace buffer. <p>NOTE: This command is not node specific.</p>
thread-statistics	Shows mdns/dlna packet statistics per thread.
<u>users</u> dlna	Shows user table.

Parameter	Description
mdns verbose	<ul style="list-style-type: none"> ▪ dlna - Shows the DLNA users. ▪ mdns - Shows the mDNS users. ▪ verbose - Shows additional information of users. <p>NOTE: This command is node specific.</p>
vlan	<p>Shows the status of all the disallowed VLANs.</p> <p>NOTE: This command is node specific.</p>

Example

The following example shows the current status of the AirGroup configuration and configured AirGroup services:

```
(host) [mynode] #show airgroup status

AirGroup Information
-----
Feature                Status
-----                -
MDNS                   Disabled
DLNA                   Enabled
Enforce Registration   Disabled
IPV6                   Enabled

AirGroup Service Information
-----
Service                Status
-----                -
remotemgmt             Disabled
DIAL                   Enabled
AmazonTV               Enabled
DLNA Media             Enabled
test                   Enabled
static                 Enabled
combined               Enabled
DLNA Print             Disabled
allowall               Enabled
sharing                Disabled
chat                   Disabled
Daniel                 Enabled
itunes                 Disabled
airplay                Enabled
airprint               Enabled
googlecast             Enabled
```

The following example displays the packets sent and received per second by AirGroup:

(host) [mynode] #show airgroup internal-state statistics

Time: Tue Jul 12 13:18:24 2016

MDNS Messages

```
-----
Opcode Name                               Sent Since Last Read  Sent Total  Recv
Since Last Read  Recv Total
-----  ----  -----
7         app                               0                               5           0
-         SDN                               0                               11090        0
Rx        Request                          N/A                             N/A          0
         591
Rx        Response                          N/A                             N/A          0
         556
Tx        Request-Refresh                    0                               10104        N/A
         N/A
Tx        Request-discovery                  0                               1836         N/A
         N/A
Tx        Request-wildcard                    0                               0            N/A
         N/A
Tx        Response-Solicited                  0                               0            N/A
         N/A
Tx        Response-Solicited-Fragment        0                               0            N/A
         N/A
Tx        Response-Unsolicited                0                               0            N/A
         N/A
Tx/Rx     Total                              0                               0            N/A
         N/A
```

DLNA Messages

```
-----
Opcode Name                               Sent Since Last Read  Sent Total  Recv Since Last
Read  Recv Total
-----  ----  -----
-         SDN                               0                               365947        0
         966861
Rx        Query                             N/A                             N/A          0
         837484
Rx        Notify Announce                    N/A                             N/A          0
         69450
Rx        Notify Bye                          N/A                             N/A          0
         6
Tx        Response                             0                               33958        N/A
         N/A
```

Internal MDNS Statistics

```
-----
Functionality                               Hit Count Since Last Read  Hit Count Total
-----
Response - Cache Update                     0                               3176
Response                                     0                               556
Query - prepare records + Policy            0                               591
```

Query - Policy	0	12
Query - resp pkt gen & send	0	0
Query - Response packet send	0	331139
Query	0	591
Multicast Response propagate	0	0

Internal DLNA Statistics

Functionality	Hit Count Since Last Read	Hit Count Total
Response - Cache Update	0	73921
Response	0	0
Query - prepare records + Policy	0	14227
Query - Policy	0	34360
Query - resp pkt gen & send	0	14170
Query - Response packet send	0	74397
Query	0	837484

MDNS Multi-controller Cluster Messages

Type	Sent Since Last Read	Sent Total	Recv
Unicast Response with tag	0	0	0
Request with tag	0	0	0
Raw Response	0	0	0
Multicast Propagate Raw Response	0	0	0

DLNA Multi-controller Cluster Messages

Type	Sent Since Last Read	Sent Total	Recv Since Last Read
Request with tag	0	0	0
Raw Response	0	0	0

Packet Arrival Statistics (per minute)

Peak Packet Arrival Rate	Peak Arrival Time	No. Servers	No. Clients
454	Jul 05 10:34:42	5	16

Cache Bucket Size

Service	AP Name Bucket	AP FQLN Bucket	User Name Bucket	Default Bucket
MDNS	0	0	0	1
SSDP	0	0	0	4

Internal mDNS and DLNA Thread Statistics

```

-----
# Thread ID Query since Last Read Queries Recv Total Queries in Queue
Peak Queries in Queue
-----
1 3368556288 0 488871 0 0
6
2 3343378176 0 92304 0 0
10
3 3318200064 0 74141 0 0
2
4 3293021952 0 109923 0 0
11
5 3267843840 0 72836 0 0
2

MDNS CPU and Throttling details
-----
Current CPU Utilization (%) Throttling State Description Query
Pkt Dropped Resp Pkt Dropped
-----
0.04(3) MDNS_NO_THROTTLING No packets dropped 0
0

list of controllers in same vlan
-----
Controller MAC
-----
00:1a:1e:01:ae:28
00:0b:86:b5:15:97
00:1a:1e:01:99:e0
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bf:70
00:1a:1e:02:07:b0
00:0b:86:9a:4e:77
00:0c:29:10:8c:b8
00:0b:86:b8:e1:d8
00:1a:1e:01:bd:b0

list of local controllers with AirGroup devices
-----
Controller MAC
-----
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bd:b0

AirGroup users 13, AirGroup servers 5. Total devices 38

```

The following example displays the DLNA packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics dlna
```

Time: Tue Jul 12 13:24:01 2016

DLNA Messages

Opcode	Name	Sent Since Last Read	Sent Total	Recv Since Last
Read	Recv Total			
-	SDN	149	366096	396
Rx	967257 Query	N/A	N/A	378
Rx	837862 Notify Announce	N/A	N/A	10
Rx	69460 Notify Bye	N/A	N/A	0
Tx	6 Response	0	33958	N/A
	N/A			

Internal DLNA Statistics

Functionality	Hit Count Since Last Read	Hit Count Total
Response - Cache Update	10	73931
Response	0	0
Query - prepare records + Policy	0	14227
Query - Policy	0	34360
Query - resp pkt gen & send	0	14170
Query - Response packet send	10	74407
Query	378	837862

DLNA Multi-controller Cluster Messages

Type	Sent Since Last Read	Sent Total	Recv Since Last Read
Recv Total			
Request with tag	0	0	0
Raw Response	0	0	0

Packet Arrival Statistics (per minute)

Peak Packet Arrival Rate	Peak Arrival Time	No. Servers	No. Clients
454	Jul 05 10:34:42	5	16

Cache Bucket Size

Service	AP Name Bucket	AP FQLN Bucket	User Name Bucket	Default Bucket
SSDP	0	0	0	4

Internal DLNA Thread Statistics

```

# Thread ID Query since Last Read Queries Recv Total Queries in Queue
Peak Queries in Queue
-----
1 3368556288 180 489051 0
6
2 3343378176 60 92216 0
10
3 3318200064 36 73770 0
2
4 3293021952 54 109965 0
11
5 3267843840 48 72860 0
2

MDNS CPU and Throttling details
-----
Current CPU Utilization (%) Throttling State Description Query
Pkt Dropped Resp Pkt Dropped
-----
0.03(3) MDNS_NO_THROTTLING No packets dropped 0
0

```

The following example displays the mDNS packets sent and received per second by AirGroup:

```

(host) [mynode] #show airgroup internal-state statistics mdns

Time: Tue Jul 12 13:26:03 2016
MDNS Messages
-----
Opcode Name Sent Since Last Read Sent Total
Recv Since Last Read Recv Total
-----
7 app 0 5
0 SDN 2 11092
0 Request 4152 N/A
Rx Request 591 N/A
Rx Response 556 N/A
Tx Request-Refresh 2 10106
N/A N/A
Tx Request-discovery 0 1836
N/A N/A
Tx Request-wildcard 0 0
N/A N/A
Tx Response-Solicited 0 0
N/A N/A

```

Tx	Response-Solicited-Fragment	0	0
N/A	N/A		
Tx	Response-Unsolicited	0	0
N/A	N/A		
Tx/Rx	Total	2	0
N/A	N/A		

Internal MDNS Statistics

Functionality	Hit Count	Since Last Read	Hit
Count Total			
Response - Cache Update	0		3176
Response	0		556
Query - prepare records + Policy	0		591
Query - Policy	0		12
Query - resp pkt gen & send	0		0
Query - Response packet send	232		331371
Query	0		591
Multicast Response propagate	0		0

MDNS Multi-controller Cluster Messages

Type	Recv Since Last Read	Recv Total	Sent Since Last Read	Sent Total
Unicast Response with tag	0		0	0
Request with tag	0		0	0
Raw Response	0		0	0
Multicast Propagate Raw Response	0		0	0

Packet Arrival Statistics (per minute)

Peak Packet Arrival Rate	Peak Arrival Time	No. Servers	No. Clients
454	Jul 05 10:34:42	5	16

Cache Bucket Size

Service Bucket	AP Name Bucket	AP FQLN Bucket	User Name Bucket	Default
MDNS	0	0	0	1

Internal MDNS Thread Statistics


```

# Thread ID  Query since Last Read  Queries Recv Total  Queries in
Queue  Peak Queries in Queue
-----
1  3368556288  0  0  0
   6
2  3343378176  0  148  0
   10
3  3318200064  0  407  0
   2
4  3293021952  0  12  0
   11
5  3267843840  0  24  0
   2

MDNS CPU and Throttling details
-----
Current CPU Utilization (%)  Throttling State  Description
Query Pkt Dropped  Resp Pkt Dropped
-----
0.02(3)  MDNS_NO_THROTTLING  No packets dropped
0  0

```

The following example displays the detailed statistics of packets sent and received per second by AirGroup:

```

(host) [mynode] ##show airgroup internal-state statistics verbose

Time: Tue Jul 12 13:27:59 2016
PAPI Messages
-----
Msg ID  Name  Sent Since last Read  Sent Total  Recv Since
Last Read  Recv Total
-----
7062  Set switch ip6  0  0  0
   1
7064  Set vlan ipv6 info  0  0  0
   1
65534  sapi getstate response  0  0  0
   1
7005  Set switch ip  0  0  0
   1
14001  mdns cli request  0  0  1
   331

RADIUS Client Messages
-----
Type  Sent Since Last Read  Sent Total  Recv Since Last
Read  Recv Total

```

```

-----
-----
Auth Req/Resp          0          30223      0
    13823
RFC3576                N/A          N/A        0
    0
CPPM Device-Entry Added N/A          N/A        0
    2
CPPM Device-Entry Deleted N/A          N/A        0
    0

```

MDNS Messages

```

-----
Opcode Name                Sent Since Last Read  Sent Total  Recv
Since Last Read  Recv Total
-----  ----
-----  -----
7      app                0                5          0
-      SDN                0                11092      0
      4152
Rx     Request            N/A             N/A        0
      591
Rx     Response           N/A             N/A        0
      556
Tx     Request-Refresh    0                10106     N/A
      N/A
Tx     Request-discovery  0                1836      N/A
      N/A
Tx     Request-wildcard   0                0          N/A
      N/A
Tx     Response-Solicited 0                0          N/A
      N/A
Tx     Response-Solicited-Fragment N/A             0          N/A
      N/A
Tx     Response-Unsolicited 0                0          N/A
      N/A
Tx/Rx  Total                0                0          N/A
      N/A

```

DLNA Messages

```

-----
Opcode Name                Sent Since Last Read  Sent Total  Recv Since Last
Read  Recv Total
-----  ----
-----  -----
-      SDN                0                366195    8
    967567
Rx     Query              N/A             N/A        8
    838110
Rx     Notify Announce    N/A             N/A        0
    69490
Rx     Notify Bye          N/A             N/A        0
    6
Tx     Response            0                33958     N/A
    N/A

```

Internal MDNS Statistics

Functionality	Hit Count Since Last Read	Hit Count Total
Response - Cache Update	0	3176
Response	0	556
Query - prepare records + Policy	0	591
Query - Policy	0	12
Query - resp pkt gen & send	0	0
Query - Response packet send	0	331387
Query	0	591
Multicast Response propagate	0	0

Internal DLNA Statistics

Functionality	Hit Count Since Last Read	Hit Count Total
Response - Cache Update	0	73961
Response	0	0
Query - prepare records + Policy	0	14227
Query - Policy	0	34360
Query - resp pkt gen & send	0	14170
Query - Response packet send	0	74437
Query	8	838110

MDNS Multi-controller Cluster Messages

Type	Sent Since Last Read	Recv Total	Sent Total	Recv
Unicast Response with tag	0	0	0	0
Request with tag	0	0	0	0
Raw Response	0	0	0	0
Multicast Propagate Raw Response	0	0	0	0

DLNA Multi-controller Cluster Messages

Type	Sent Since Last Read	Sent Total	Recv Since Last Read	Recv Total
Request with tag	0	0	0	0
Raw Response	0	0	0	0

Packet Arrival Statistics (per minute)

Peak Packet Arrival Rate	Peak Arrival Time	No. Servers	No. Clients
454	Jul 05 10:34:42	5	16

Cache Bucket Size

Service	AP Name Bucket	AP FQLN Bucket	User Name Bucket	Default Bucket
MDNS	0	0	0	1
SSDP	0	0	0	4

Internal mDNS and DLNA Thread Statistics

#	Thread ID	Query since Last Read	Queries Recv Total	Queries in Queue
1	3368556288	2	489191	0
2	3343378176	4	92394	0
3	3318200064	0	74189	0
4	3293021952	0	110019	0
5	3267843840	2	72908	0

MDNS CPU and Throttling details

Current CPU Utilization (%)	Throttling State	Description	Query
0.03(3)	MDNS_NO_THROTTLING	No packets dropped	0

list of controllers in same vlan

Controller MAC

```

00:1a:1e:01:ae:28
00:0b:86:b5:15:97
00:1a:1e:01:99:e0
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bf:70
00:1a:1e:02:07:b0
00:0b:86:9a:4e:77
00:0c:29:10:8c:b8
00:0b:86:b8:e1:d8
00:1a:1e:01:bd:b0
    
```

list of local controllers with AirGroup devices

Controller MAC

```

00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bd:b0
    
```

AirGroup users 10, AirGroup servers 5. Total devices 36

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show airgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.7.0.0	New sub-parameter <code>ppm</code> is added to the <code>internal-state statistics</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup active-domains

```
show airgroup active-domains
```

Description

This command shows the list of configured AirGroup active-domains. This command is applicable only on stand-alone controllers.

Example

The following example shows the list of configured AirGroup active-domains:

```
(host) [mynode] #show airgroup active-domains

AirGroup Active-Domains
-----
Domain Name  Status
-----
Campus1     Included
Campus2     Included

Num active-domains:2
```

The output of this command includes the following parameters:

Parameter	Description
Domain Name	Shows the name of the domain.
Status	Shows the status of the domain if it is part of the active-domain list.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.

Command	Description
show airgroup	This command shows the global AirGroup settings.
show airgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on stand-alone controller.

show airgroup aps

show airgroup aps

Description

This command shows the AP tables.

Example

The following example shows the AP tables:

```
(host) [mynode] #show airgroup aps

AirGroup APs
-----
IP   Name      Group      MAC          BSSID- A      BSSID- B/G
--   -
AP102  apgrp-clust ac:a3:1e:c7:71:2e ac:a3:1e:f7:12:f0 ac:a3:1e:f7:12:e0
7010AP apgrp-clust ac:a3:1e:ca:7e:04 ac:a3:1e:27:e0:50 ac:a3:1e:27:e0:40

FQLN Neighbor count- A Neighbor count- B/G Neighbor AP name BAND
-----
      3              3              alpha            A
                        ac:a3:1e:27:e0:50 A
                        beta              A
      3              2              ac:a3:1e:cf:b9:90 A
                        gamma             A
                        40:e3:d6:bf:65:50 A

Num APs:3
```

The output of this command includes the following parameters:

Column	Description
IP	Shows the IP address of the AirGroup AP.
Name	Shows the name of the AP.
Group	Shows the group of the AirGroup user.
MAC	Shows the MAC address of the AirGroup AP.
BSSID- A	Shows the BSSID-A of the AirGroup AP.
BSSID- B/G	Shows the BSSID-B/G of the AirGroup AP.

Column	Description
FQLN	Shows the FQLN of the AirGroup AP.
Neighbor count- A	Shows the neighbor count-A of the AirGroup AP.
Neighbor count- B/G	Shows the neighbor count-B/G of the AirGroup AP.
Neighbor AP name	Shows the name of the neighbor AP (if available) or the BSSID of the neighbor AP.
BAND	Shows the band of the AirGroup AP.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.4.0.0	Updated the description of parameter, Neighbor AP name.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup blocked-queries

```
show airgroup blocked-queries [dlna|mdns]
```

Description

This command shows the service ID that was queried but not available in the AirGroup service table.

Parameter	Description
dlna	Shows the DLNA blocked queries.
mdns	Shows the mDNS blocked queries.

Example

The following example displays the service ID that was queried but not available in the AirGroup service table:

```
(host) [mynode] #show airgroup blocked-queries

AirGroup dropped Query IDs
-----
Service ID                                     #query-hits  Thread Num
-----
urn:schemas-wifi-ally-urn:device:WFADevice:1    9            1
urn:schemas-upnp-org:device:InternetGatewayDevice:1 485113       1
_appletv._tcp                                     60           2
_sleep-proxy._udp                                 64           2
urn:schemas-wifi-ally-urn:device:WFADevice:1    672          2
_airport._tcp                                     60           2
_appletv-pair._tcp                               60           2
_touch-remote._tcp                              60           2
urn:schemas-upnp-org:device:InternetGatewayDevice:1 90476        2
_appletv._tcp                                     60           3
_sleep-proxy._udp                                 86           3
_airport._tcp                                     146          3
_appletv-pair._tcp                               60           3
_touch-remote._tcp                              60           3
urn:schemas-upnp-org:device:InternetGatewayDevice:1 73056        3
urn:schemas-wifi-ally-urn:device:WFADevice:1    36           4
urn:schemas-upnp-org:device:InternetGatewayDevice:1 93141        4
urn:schemas-wifi-ally-urn:device:WFADevice:1    12           5
urn:schemas-upnp-org:device:InternetGatewayDevice:1 72176        5
Num dropped Query IDs:19
```

The output of this command includes the following parameters:

Column	Description
Service ID	Shows the service ID that was queried but not available in the AirGroup service table.
#query-hits	Shows the number of query hits for a service blocked by AirGroup.
Thread Num	Shows the thread number of the service ID.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup blocked-service-id

```
show airgroup blocked-service-id [dlna|mdns]
```

Description

This command shows the list of blocked services.

Parameter	Description
dlna	Specifies the DLNA blocked services.
mdns	Specifies the mDNS blocked services.

Example

The following example shows the list of blocked services:

```
(host) [mynode] #show airgroup blocked-service-id

AirGroup Blocked Service IDs
-----
Origin                Service ID                #response-hits
-----
fe80::6203:8ff:fe94:74a6  _sftp-ssh._tcp           82
fe80::6203:8ff:fe94:74a6  _ssh._tcp                 82
10.16.124.236             _uscan._tcp               40
10.16.126.248             _keepalive._dns-sd._udp  20
Num Blocked Service-ID:4
```

The output of this command includes the following parameters:

Column	Description
Origin	Shows the source IP address of the AirGroup server that advertises this service.
Service ID	Shows the blocked service ID of the server.
#response-hits	Shows the number of response messages received for this service ID.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup cache entries

```
show airgroup cache entries [debug|dlna|mac|mdns|static|verbose]
```

Description

This command shows the AirGroup mDNS and DLNA resource records in cache.

Parameter	Description
debug	Shows debug information.
dlna	Shows the DLNA cache entries.
mac	Shows entries filtered on a specific MAC address of the server.
mdns	Shows the mDNS cache entries.
static	Shows static cache entries.
verbose	Shows details cache entries.

Example

The following example shows the AirGroup mDNS resource records in the cache:

```
(host) [mynode] #show airgroup cache entries mnds

Cache Entries
-----
Name                Type  Class  TTL   Origin  Expiry  Last Update
-----
world_cricket       A     IN     120   0.0.0.0  static  N/A
_icct20._tcp.local PTR   IN     4500  0.0.0.0  static  N/A
Num Cache Entries:2
```

The output of this command includes the following parameters:

Column	Description
Name	Shows the name of the Service ID.
Type	Shows the type of mDNS or DLNA record.
Class	Shows the class of the record. This is usually IN.

Column	Description
TTL	Shows the time to live value of the service ID in seconds.
Origin	Shows the source IP of the AirGroup server.
Expiry	Shows the expiry period of the mDNS or DLNA record in seconds.
Last Update	Shows the time stamp of the last cache update.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup cppm

show airgroup cppm [entries|server-group]

Description

This command shows information for devices registered in ClearPass Policy Manager.

Parameter	Description
entries	Shows the ClearPass Policy Manager registration information.
server-group	Shows the Server Group information.

Example

The following example shows the information for devices registered in ClearPass Policy Manager:

```
(host) [mynode] #show airgroup cppm entries

ClearPass Guest Device Registration Information
-----
Device          device-owner  shared location-id AP-name  shared
location-id AP-FQLN
-----
cc:3a:61:b1:4a:cc  lecturer
c4:85:08:a2:15:1b  N/A
00:1e:65:2d:ae:44  N/A

shared location-id AP-group  shared user-list  shared group-list  shared
role-list  CPPM-Req  CPPM-Resp
-----
          lecturer2
          1          1          DEPT1
          1          1          Physics
          1          1          Chemistry

Num CPPM Entries:3
```

The output of this command includes the following parameters:

Column	Description
Device	Shows the MAC address of the AirGroup device.
device-owner	Shows the user name of the AirGroup device.
shared location-id AP-name	Shows the location ID based on AP name.
shared location-id AP-FQLN	Shows the location ID based on the FQLN value of an AP.
shared location-id AP-group	Shows the location ID based on the name of an AP group.
shared user-list	Shows one or more primary login IDs of an AirGroup user.
shared group-list	Shows one or more primary login IDs of an AirGroup user group.
shared role-list	Shows the name of the role.
CPPM-Req	Shows the number of requests sent to ClearPass Policy Manager to populate the policy details for the given client.
CPPM-Resp	Shows the number of responses received from the ClearPass Policy Manager for the policy details of the given client.

The following example shows the server group information:

```
(host) [mynode] #show airgroup cppm server-group

Airgroup AAA Server Group
-----
Name    Inservice  trim-FQDN  match-FQDN
-----  -
cppm    Yes        No
```

The output of this command includes the following parameters:

Parameter	Description
Name	Shows server group name.
Inservice	Shows in service status of server group.
trim-FQDN	Shows trim FQDN status of server group.
match-FQDN	Shows matching FQDN of server group.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.11.0.0	The flag, D was introduced in the output of the command to indicate that the servers share the same username.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup cppm-server

```
show airgroup cppm-server {aaa|query-interval|radius statistics|rfc3576 statistics}
```

Description

This command shows the ClearPass Policy Manager server information.

Parameter	Description
<aaa>	Shows AirGroup aaa profile.
query-interval	Shows the ClearPass Policy Manager periodic query interval time. 1 - 24 hours 10 hours
radius statistics	Shows the RADIUS server statistics for AirGroup.
rfc3576 statistics	Shows the RFC3576 server statistics for AirGroup.

Example

The following example shows the AirGroup aaa profile information:

```
(host) [mynode] #show airgroup cppm-server aaa

Airgroup AAA profile
-----
Parameter                               Value           Set
-----
Server Group                             san-dot1x
RFC 3576 server                           10.15.16.39
Configure dead time for a down Server     5
Configure UDP port to receive RFC 3576 server requests. 5999
```

The output of this command includes the following parameters:

Column	Description
Parameter	Shows the parameter name.
Value	Shows the value configured.
Set	Shows the value applied.

The following example shows the ClearPass Policy Manager query interval:

```
(host) [mynode] #show airgroup cppm-server query-interval

CPPM Server Query Interval
-----
Timer Value  Unit
-----  ----
10           hours
```

The output of this command includes the following parameters:

Column	Description
Timer Value	Shows the query interval.
Unit	Shows the unit of the query interval.

The following example shows the RADIUS server statistics:

```
(host) [mynode] #show airgroup cppm-server radius statistics

Airgroup RADIUS Server Statistics
-----
Statistics          cppm_ser01
-----
PAP Requests        30175
Mismatch Response   1070
Bad Authenticator    0
Access-Accept       29032
Access-Reject       7
Unknown Response code 0
Timeouts            6906
AvgRespTime (ms)    815
Total Requests      30175
Total Responses     30109
Uptime (d:h:m)      0:2:19
SEQ Total/Free      255/255
Orphaned requests = 0
The following example shows the RFC3576 server statistics:
(host) [mynode] #show airgroup cppm-server rfc3576 statistics

Airgroup RFC3576 Statistics
-----
Statistics          10.15.16.39
-----
Disconnect Requests 0
No Secret            0
Bad Authenticator    0
Invalid Request      0
Packets Dropped      0
Unknown service      0
```

```

CoA Requests          0
CoA Accepts          0
CoA Rejects          0
No permission         0
RFC3576 port number      : 5999
Packets received from unknown clients : 0
Packets received with unknown request : 0
Total RFC3576 packets Received      : 0

```

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup domain

show airgroup domain

Description

This command shows the list of configured AirGroup domains. This command is applicable only on stand-alone controllers.

Example

The following example shows the list of configured AirGroup domains:

```
(host) [mynode] #show airgroup domain

AirGroup Domains
-----
Name  Description  IP-Address
----  -
test  test         10.15.52.2
10.15.52.16
ag    10.15.52.2
10.15.52.16
Num domains:2
```

The output of this command includes the following parameters:

Column	Description
Name	Shows the name of the AirGroup domain.
Description	Shows a short description of the AirGroup domain.
IP-Address	Shows IP address or VRRP IP address the stand-alone controller.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.

Command	Description
show airgroup	This command shows the global AirGroup settings.
show airgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on stand-alone controller.

Column	Description
Flow Grp ID	Shows flow group ID information.
Flow ID	Shows the flow ID information.
In Port	Shows the in port information.
Src Mac	Shows the source MAC address.
Dst Mac	Shows the destination MAC address.
Ether	Shows the Ether information.
Src IP	Shows the source IP address.
Dst IP	Shows the destination IP address.
Proto	Shows the protocol information.
Src Port	Shows the source port information.
Dst Port	Shows the destination port information.
Actions	Shows the applied actions.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airgroup multi-controller-table

```
show airgroup multi-controller-table [dlna|mdns|verbose]
```

Description

This command shows the information of all stand-alone controllers participating in an AirGroup domain. This command is applicable only on stand-alone controllers.

Parameter	Description
dlna	Shows the DLNA statistics.
mdns	Shows the mDNS statistics.
verbose	Shows the detailed statistics.

Example

The following example shows information of all stand-alone controllers participating in an AirGroup domain:

```
(host) [mynode] #show airgroup multi-controller-table

AirGroup Multi-Controller-Table
-----
IP-Address
-----
10.15.52.16
Num IP-Address:1
The following example shows the DLNA statistics all stand-alone controllers
participating in an AirGroup domain:
(host) [mynode] #show airgroup multi-controller-table dlna

AirGroup Multi-Controller-Table verbose
-----
IP-Address   Type   Request with Tag Tx   Unicast Response with tag Tx   Raw
Response Tx   Request with Tag Rx   Unicast Response with tag Rx   Raw Response
Rx
-----
-----
-
10.15.52.16  DLNA   448                   N/A                               0
              0                   N/A                               0
Num IP-Address:1
The following example shows the mDNS statistics all stand-alone controllers
participating in an AirGroup domain:
(host) [mynode] #show airgroup multi-controller-table mdns
```

```

AirGroup Multi-Controller-Table verbose
-----
IP-Address   Type  Request with Tag Tx  Unicast Response with tag Tx  Raw
Response Tx  Request with Tag Rx  Unicast Response with tag Rx  Raw Response
Rx
-----
-
10.15.52.16  mDNS  1134                0                               0
0
Num IP-Address:1

```

The following example shows the detailed statistics all stand-alone controllers participating in an AirGroup domain:

```

(host) [mynode] #show airgroup multi-controller-table verbose

AirGroup Multi-Controller-Table verbose
-----
IP-Address   Type  Request with Tag Tx  Unicast Response with tag Tx  Raw
Response Tx  Request with Tag Rx  Unicast Response with tag Rx  Raw Response
Rx
-----
-
10.15.52.16  mDNS  1134                0                               0
0
10.15.52.16  DLNA  448                N/A                             0
0
Num IP-Address:1

```

The output of this command includes the following parameters:

Table 11: *show airgroup multi-controller-table*

Column	Description
IP-Address	Shows the IP address of all stand-alone controllers participating in an AirGroup domain.
Type	Shows the type of record.
Request with Tag Tx	Shows the number of AirGroup queries transmitted with meta-tag information.
Unicast Response with tag Tx	Shows the number of AirGroup responses transmitted with meta-tag information.
Raw Response Tx	Shows the number of mDNS or DLNA responses transmitted.

Column	Description
Request with Tag Rx	Shows the number of AirGroup queries received with meta-tag information.
Unicast Response with tag Rx	Shows the number of AirGroup responses received with meta-tag information.
Raw Response Rx	Shows the number of mDNS or DLNA responses received.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on stand-alone controllers.

show airgroup policy-entries

```
show airgroup policy-entries [mac {neighborhood <macaddr>}|<macaddr>]
```

Description

This command shows active AirGroup policies.

Parameter	Description
mac neighborhood <macaddr>	Shows AP neighborhood to discover the AirGroup server.
mac <macaddr>	Shows active AirGroup policies for the specified MAC address.

Example

The following example shows the active AirGroup policies:

```
(host) [mynode] #show airgroup policy-entries

AirGroup Device Policy Information
-----
Device          device-owner  shared location-id AP-name  shared
location-id AP-FQLN
-----
aa:aa:aa:aa:aa:aa  N/A
aa:bb:cc:dd:ee:ff  N/A          xyzzy

shared location-id AP-group  shared user-list  shared group-list  shared
role-list
-----
                                sy          saasa
                                test

CPPM-Req  CPPM-Resp  source  Auto-Associate  Neighborhood
-----  -
                                CLI          1 hop(s)
                                CLI          AP-Name      1 hop(s)

Num Policy Entries:2
```

The output of this command includes the following parameters:

Column	Description
Device	Shows the MAC address of the device.
device-owner	Shows the device owner information.
shared AP-name	Shows the shared AP name information.
shared AP-FQLN	Shows the shared AP FQLN information.
shared AP-group	Shows the shared AP group information.
shared users	Shows the shared user information.
shared groups	Shows the shared group information.
shared roles	Shows the shared roles information.
CPPM-Req	Shows the ClearPass Policy Manager requests.
CPPM-Resp	Shows the ClearPass Policy Manager responses.
source	Shows the source (CLI or ClearPass Policy Manager) of the policy.
Auto-associate	Shows the auto association information.
Neighborhood	Shows the neighborhood information.

The following example shows the AP neighborhood to discover the AirGroup server by using a specific MAC address:

```
(host) [mynode] #show airgroup policy-entries mac 00:1a:1e:aa:bb:cc

AirGroup Device Policy Information
-----
Device          device-owner  shared location-id AP-name  shared
location-id AP-FQLN
-----
00:1a:1e:aa:bb:cc  N/A

shared location-id AP-group  shared user-list  shared group-list  shared
role-list
-----
test

CPPM-Req  CPPM-Resp  source  Auto-Associate  Neighborhood
-----
CLI  1 hop(s)
```

```
Num Policy Entries:1
```

The output of this command includes the following parameters:

Column	Description
Device	Shows the MAC address of the device.
device-owner	Shows the device owner information.
shared AP-name	Shows the shared AP name information.
shared AP-FQLN	Shows the shared AP FQLN information.
shared AP-group	Shows the shared AP group information.
shared users	Shows the shared user information.
shared groups	Shows the shared group information.
shared roles	Shows the shared roles information.
CPPM-Req	Shows the ClearPass Policy Manager requests.
CPPM-Resp	Shows the ClearPass Policy Manager responses.
source	Shows the source (CLI or ClearPass Policy Manager) of the policy.
Auto-associate	Shows the auto association information.
Neighborhood	Shows the neighborhood information.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airgroup query-result

```
show airgroup query-result {excluded}| {mac <server mac address>
```

Description

This command shows the list of AirGroup servers that are available and excluded for a client.



This command should be executed only after issuing the `airgroup send-query` command.

Parameter	Description
<code>excluded</code>	Shows the list of servers that are excluded for a client.
<code>mac <server mac address></code>	Shows the AirGroup server information of a specific MAC address.

Example

The following example displays the AirGroup query result:

```
(host) [mynode] #show airgroup query-result

Query result generated:
Timestamp :: 2022-08-09 21:08:55
Client :: 00:8e:9b:00:00:00
Service-id :: _airplay_tcp
AP Name :: APSim04_000_000
User name :: user1
User role :: authenticated
User group :: -
VLAN ID :: 50
```

CPPM State: Done - CPPM request done; Fail - CPPM Request failed; No policy - No Policy in Clearpass; NR - Not required; Req 1/2/3 - Request Attempt number; Global CPPM State -

Req 3 Flags: A - AP location; C - CPPM policy; D - Entry added with username based auto tag feature; M - MD location; R - Cluster location; S - AP Mcast server; U - Unknown location;

AirGroup Servers Included

MAC	IP	Type	Host Name	Service
---	--	----	-----	-----
00:8e:9b:00:00:07	50.1.0.9	mDNS,DLNA	sim_sta_000_007-APPLETVS	default-allowall
00:8e:9b:00:00:08	50.1.0.10	mDNS,DLNA	sim_sta_000_008-APPLETVS	default-allowall

VLAN	Wired/Wireless	Role	Group	Username	AP-Name
---	-----	----	-----	-----	-----
50	Wireless	authenticated	-	user1	APSim04_000_000
50	Wireless	authenticated	-	user1	APSim04_000_000

AP-Group	CPPM State	CoA Count	Controller-MAC	Flags	Index
-----	-----	-----	-----	-----	---
AP_groupAPSim040	No Policy	0	00:0c:29:0c:3e:0b	A	14
AP_groupAPSim040	Done	0	00:0c:29:0c:3e:0b	AC	51

Number of AirGroup servers: 2

The following example displays the output of the show airgroup query-result excluded command:

```
(host) [md] #show airgroup query-result excluded
Query result generated:
Timestamp :: 2022-08-09 21:08:55
Client :: 00:8e:9b:00:00:00
Service-id :: _airplay._tcp
AP Name :: APSim04_000_000
User name :: user1
User role :: authenticated
User group :: -
VLAN ID :: 50
CPPM State: Done - CPPM request done; Fail - CPPM Request failed; No policy
- No Policy in Clearpass; NR - Not required; Req 1/2/3 - Request Attempt
number;
Global CPPM State - Req 1 Flags: A - AP location; C - CPPM policy; D -
Entry added with username based auto tag feature; M - MD location; R -
Cluster location;
S - AP Mcast server; U - Unknown location;

AirGroup Servers Included
-----
```

```

MAC                IP            Type      Host Name          Service
---                --            -
00:8e:9b:00:00:0b  50.1.0.13   mDNS     sim_sta_000_011-APPLETVS  default-allowall
00:8e:9b:00:00:0c  50.1.0.14   mDNS     sim_sta_000_012-APPLETVS  default-allowall

VLAN  Wired/Wireless  Role          Group  Username  AP-Name
----  -
50    Wireless        authenticated -      user1     APsim04_000_000
50    Wireless        authenticated -      user1     APsim04_000_000

AP-Group          CPPM State    CoA Count  Controller-MAC      Flags  Index
-----
AP_groupAPsim040  No Policy    0          00:0c:29:0c:3e:0b  A      69
AP_groupAPsim040  No Policy    0          00:0c:29:0c:3e:0b  A      22
Number of AirGroup servers: 2

```

The following example displays the query result of a specific MAC address:

```

(host) [md] #show airgroup query-result mac 00:8e:9b:00:00:0a
Query result generated:
Timestamp :: 2022-08-09 21:08:55
Client :: 00:8e:9b:00:00:00
Service-id :: _airplay._tcp
AP Name :: APsim04_000_000
User name :: user1
User role :: authenticated
User group :: -
VLAN ID :: 50
AirGroup Server Information 00:8e:9b:00:00:0a
Tid :: 4
index :: 61
mac :: 00:8e:9b:00:00:0a
Ip Address :: 50.1.0.12
Host Name :: sim_sta_000_010-APPLETVS
User Name :: user1
VLAN :: 50
User role :: authenticated
Type :: mDNS
Wired/Wireless :: Wireless
AP :: 00:d8:65:00:00:00
Group Name :: AP_groupAPsim040
AP Name :: APsim04_000_000
Group :: -
CPPM State :: Done
CPPM Expiry :: 2389
CoA Count :: 0
MD mac :: 00:0c:29:0c:3e:0b
Transport Out Port :: 18 (00:0c:29:0c:3e:0b)
Is OFA Port dirty :: SDN PORT LOOKUP DONE

```

```
Service Name      :: default-allowall
Server created time :: Tue Aug  9 21:08:05 2022
Last Advertisement Received :: Tue Aug  9 21:08:05 2022
MDNS Packet In Total :: 1
MDNS Packet In Last Minute :: 0
DLNA Packet In Total :: 0
DLNA Packet In Last Minute :: 0
```

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode.

show airgroup servers

```
show airgroup servers
  debug
  dlna
  location <ap-group | ap-name | cluster | unknown>
  mac
  mdns
  username <username>
  verbose
```

Description

This command shows the list of AirGroup servers.

Parameter	Description
debug	Shows server debug information.
dlna	Shows the DLNA servers.
mac <macaddr>	Shows entries filtered on a specific MAC address of the server.
mdns	Shows the mDNS servers.
location	Shows the list of AirGroup servers based on the location.
ap-group	Shows the details of AirGroup servers mapped to an AP group,
ap-name	Shows the details of AirGroup servers mapped to an AP.
cluster	Shows the details of AirGroup servers mapped to a cluster.
unknown	Shows the list of servers for which the location is unknown.
username <username>	Shows the list of servers that share the same username
verbose	Shows the detailed statistics.

Example

The following example shows the list of AirGroup servers:

```

(host) [mynode] #show airgroup servers

AirGroup Servers
-----
MAC                IP                Type  Host Name        Service
---                --                ----  -
5c:aa:fd:52:5a:f8  10.16.124.224    DLNA  world_cricket    allowall
                    10.16.124.226    DLNA  world_cricket    DLNA Media
5c:aa:fd:52:5a:fa  10.16.124.226    DLNA  world_cricket    DLNA Media
                    10.16.126.16     DLNA  world_cricket    allowall
f0:4d:a2:83:74:a5  10.16.126.16     DLNA  world_cricket    DLNA Media
                    0.0.0.0           mDNS  world_cricket    allowall
11:11:11:11:11:11  0.0.0.0           mDNS  world_cricket    static
a0:02:dc:85:c2:98  10.16.124.181    DLNA  10-16-124-181    DIAL

VLAN  Wired/Wireless  Role      Group  Username  AP-Name
----  -
124   wireless        ipad      -
124   wireless        ipad      -
126   N/A
0     N/A
124   wireless        x86-role  -      arr

Num Servers: 5.

```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. NOTE: The column displays Wired when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays N/A .
Role	Shows the user role of the AirGroup server.

Column	Description
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the list of AirGroup servers hosting DLNA service:

```
(host) [mynode] #show airgroup servers dlna

AirGroup Servers
-----
MAC          IP           Type  Host Name      Service
---          --          ---  -
5c:aa:fd:52:5a:f8  10.16.124.224  DLNA
5c:aa:fd:52:5a:fa  10.16.124.226  DLNA
f0:4d:a2:83:74:a5  10.16.126.16   DLNA
a0:02:dc:85:c2:98  10.16.124.181  DLNA  10-16-124-181  DIAL

VLAN  Wired/Wireless  Role      Group  Username  AP-Name
----  -
124   wireless       ipad
124   wireless       ipad
126   N/A
124   wireless       x86-role
Num Servers: 4.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.

Column	Description
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. NOTE: The column displays Wired when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays N/A .
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the list of AirGroup servers hosting mDNS service:

```
(host) [mynode] #show airgroup servers mdns

AirGroup Servers
-----
MAC                IP                Type  Host Name      Service
---                --                ---  -
11:11:11:11:11:11  0.0.0.0          mDNS  world_cricket  static

VLAN  Wired/Wireless  Role    Group  Username  AP-Name
----  -
0     N/A
Num Servers: 1.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected.

Column	Description
	NOTE: The column displays Wired when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays N/A .
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the detailed statistics of the AirGroup servers:

```
(host) [mynode] #show airgroup servers verbose

AirGroup Servers
-----
MAC                IP                Type  Host Name      Service
---                --                ---  -
5c:aa:fd:52:5a:f8  10.16.124.224   DLNA  -              allowall
                                      DLNA Media

VLAN  Wired/Wireless  Role      Group  Username
----  -
124   wireless       ipad

AP-Name  Rec-dropped  Rec-filtered  Rec-responded  Last-query
-----  -
7010AP   0            0            0

Query Throttled  Resp Throttled  CPPM-Req  CPPM-Rsp  CoA
-----  -
0          0            1          1          0

CPPM Dev-Added  CPPM Dev-Deleted  Max PPM  Max PPM at  All IP(s)
-----  -
          Controller IP
          -----
          10.16.125.117
          87          Jul 05 11:00:45  10.16.124.224

Num Servers: 5.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. NOTE: The column displays Wired when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays N/A .
VLAN	Shows the VLAN ID of the AirGroup server.
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.
Rec-dropped	Shows the number of queries dropped from the AirGroup server.
Rec-filtered	Shows the number of queries filtered as a result of the policies.
Rec-responded	Shows the number of queries responded from the AirGroup server.
Last-query	Shows the time stamp of the last query received.
CPPM-Req	Shows the number of requests sent to the ClearPass Policy Manager server to populate the policy details for the given AirGroup server.
CPPM-Rsp	Shows the number of responses received from the ClearPass Policy Manager server for policy details of the given AirGroup server.
CoA	Shows the number of Change of Authorization (CoA) requests sent by ClearPass Policy Manager server indicating the registered device.

Column	Description
CPPM Dev-Added	Shows the last time stamp when ClearPass Policy Manager policy information was learned.
CPPM Dev-Deleted	Shows the last time stamp when this device entry was deleted from the ClearPass Policy Manager table.
Max PPM	Shows the maximum PPM.
Max PPM at	Shows when the maximum PPM was reached.
All IPs	Shows all IP addresses
controller IP	Shows IP address of other stand-alone controllers.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.11.0.0	The following modifications were introduced: <ul style="list-style-type: none"> ■ The username parameter was introduced. ■ The flag, D was introduced in the output of the command to indicate that the servers share the same username.
ArubaOS 8.9.0.1	The <code>location</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airgroup status

```
show airgroup status
```

Description

This command shows the status of AirGroup.

Example

The following example shows the status of AirGroup:

```
(host) [mynode] #show airgroup status

AirGroup version: ver1

AirGroup Information
-----
Feature                Status
-----                -
MDNS                   Disabled
DLNA                   Enabled
Enforce Registration   Disabled
IPV6                   Enabled

AirGroup Service Information
-----
Service      Status
-----
remotemgmt   Disabled
DIAL         Enabled
AmazonTV     Enabled
DLNA Media   Enabled
test        Enabled
static       Enabled
combined     Enabled
DLNA Print   Disabled
allowall     Enabled
sharing      Disabled
chat        Disabled
Daniel      Enabled
itunes      Disabled
airplay     Enabled
airprint    Enabled
googlecast  Enabled
```

Starting from ArubaOS 8.11.0.0, the command displays whether the domain name has been included for username based policies:

```
(host) [mynode] #show airgroup status
```

```

Showing AirGroup info from /md
AirGroup Information
-----
Feature                Status
-----
AirGroup version      ver2
AirGroup mode         Centralized
AirGroup Profile      newestest
CPPM Profile          load-baance
Active domain         NA
Network Profile       default
MDNS                  Enabled
DLNA                  Enabled
Enforce Registration  Enabled
IPV6                  Enabled

AirGroup Service Information
-----
Service                Status
-----
default-airprint      Enabled
default-dlna-media    Enabled
default-dial          Enabled

AirGroup Profile Network Profile
-----
Max no. of servers per query:      30
Max no. of servers in location:    100
Wired Server Expiry (min):         10
Wireless Server Expiry (min):      120
Include domain for username policy: False
MAC:0
OUI:0

```

The output of this command includes the following parameters:

Column	Description
Feature	Shows name of the AirGroup feature.
Status	Shows status of the AirGroup feature.
Service	Shows name of the AirGorup service.
Status	Shows status of the AirGroup service.
AirGroup Profile Network Profile	Shows the details of AirGroup Profile Network Profile

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameter, include domain for username policy was introduced.
ArubaOS 8.8.0.0	The <code>airgroup version</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airgroup tracebuf

```
show airgroup tracebuf [msgs [ip <ipaddr>]][mac <macaddr>]]|pps]
```

Description

This command shows the trace buffer.

Parameter	Description
msgs [ip <ipaddr>]	Shows the AirGroup trace buffer for the specified IP address.
msgs [mac <macaddr>]	Shows the AirGroup trace buffer for the specified MAC address.
pps	Shows the AirGroup packet arrival trace buffer.

Example

The following example shows the trace buffer:

```
(host) [mynode] #show airgroup tracebuf

Airgroup Client(s) Message Trace
-----
Client(MAC)  Client(IP)  Time  Event
-----
Airgroup Packet Arrival Message Trace
-----
Time          Event
-----
Jul  5 10:35:42  Total Packets 454, MDNS: 0, DLNA: 0, Servers: 5, Users 16,
CPU 0.10
Jul  5 10:20:41  Total Packets 286, MDNS: 0, DLNA: 0, Servers: 5, Users 17,
CPU 0.07
Jul  5 10:17:40  Total Packets 282, MDNS: 0, DLNA: 0, Servers: 5, Users 18,
CPU 0.07
Jul  4 16:01:38  Total Packets 260, MDNS: 0, DLNA: 0, Servers: 5, Users 11,
CPU 0.07
Jul  4 16:00:37  Total Packets 222, MDNS: 0, DLNA: 0, Servers: 5, Users 9,
CPU 0.06
Jul  4 15:59:37  Total Packets 217, MDNS: 0, DLNA: 0, Servers: 5, Users 6,
CPU 0.08
Jul  4 11:29:11  Total Packets 190, MDNS: 0, DLNA: 0, Servers: 2, Users 3,
CPU 0.06
Jul  4 11:18:10  Total Packets 85, MDNS: 0, DLNA: 0, Servers: 1, Users 0,
CPU 0.03
Jul  4 11:17:10  Total Packets 6, MDNS: 0, DLNA: 0, Servers: 1, Users 0, CPU
0.00
Num Trace Entries:9
```


The output of this command includes the following parameters:

Column	Description
Client (MAC)	Shows the MAC address of the client.
Client (IP)	Shows the IP address of the client.
Time	Shows the time when the event occurred.
Event	Shows the details of the event.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup users

```
show airgroup users [mac|dlna|mdns|verbose]
```

Description

This command shows the AirGroup user table.

Parameter	Description
mac <macaddr>	Shows entries filtered on a specific MAC address of the server.
dlna	Shows the DLNA users.
mdns	Shows the mDNS users.
verbose	Shows detailed statistics.

Example

The following example shows the AirGroup users:

```
(host) [mynode] #show airgroup users

AirGroup Users
-----
MAC          IP          Type  Host Name  VLAN  Wired/Wireless  Role
Group  Username  AP-Name  -----  ----  -----
-----  -----  -----
b8:ca:3a:cb:cd:c4  10.16.126.18  DLNA          126  N/A
34:e6:d7:09:d6:41  10.16.126.25  mDNS          126  N/A
34:e6:d7:09:d7:9b  10.16.126.29  DLNA          126  N/A
f8:ca:b8:18:10:58  10.16.126.54  mDNS          126  N/A
Num Users: 4.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup user.
IP	Shows the IP address of the AirGroup user.
Type	Shows the type of the AirGroup device.

Column	Description
Host Name	Shows the host name of the AirGroup user.
VLAN	Shows the VLAN ID of the AirGroup user.
Wired/Wireless	Shows how the AirGroup user is connected.
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

The following example shows the dlna AirGroup users:

```
(host) [mynode] #show airgroup users dlna

AirGroup Users
-----
MAC          IP          Type  Host Name  VLAN  Wired/Wireless  Role
Group  Username  AP-Name
---      ---      ---
-----  -----  -----
b8:ca:3a:cb:cd:c4  10.16.126.18  DLNA          126  N/A
34:e6:d7:09:d7:9b  10.16.126.29  DLNA          126  N/A
Num Users: 2.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup user.
IP	Shows the IP address of the AirGroup user.
Type	Shows the type of the AirGroup device.
Host Name	Shows the host name of the AirGroup user.
VLAN	Shows the VLAN ID of the AirGroup user.
Wired/Wireless	Shows how the AirGroup user is connected.
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

The following example shows the mDNS AirGroup users:

```
(host) [mynode] #show airgroup users mdns

AirGroup Users
-----
MAC          IP          Type  Host Name  VLAN  Wired/Wireless  Role
Group  Username  AP-Name
-----  -----  -----  -----  -----  -----  -----
34:e6:d7:09:d6:41  10.16.126.25  mDNS          126  N/A
f8:ca:b8:18:10:58  10.16.126.54  mDNS          126  N/A
Num Users: 2.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup user.
IP	Shows the IP address of the AirGroup user.
Type	Shows the type of the AirGroup device.
Host Name	Shows the host name of the AirGroup user.
VLAN	Shows the VLAN ID of the AirGroup user.
Wired/Wireless	Shows how the AirGroup user is connected.
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show airgroup	This command shows the global AirGroup settings.
show airgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup vlan

show airgroup vlan

Description

This command shows a list of AirGroup VLANs with certain associated details such as VLAN ID, server status, and user status.

Example

The following example shows a list of AirGroup VLANs:

```
(host) [mynode] #show airgroup vlan

VLAN Table
-----
Vlan-Id  Server Status  User Status
-----
1         Allowed        Allowed
9         Allowed        Allowed
50        Allowed        Allowed
124       Allowed        Allowed
default  N/A            N/A
Num Vlans:5
```

The output of this command includes the following parameters:

Column	Description
Vlan-Id	Shows the VLAN ID.
Server Status	Shows the status of AirGroup server.
User Status	Shows the status of AirGroup user.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show airgroup	This command shows the global AirGroup settings.
show airgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode.

show airgroupprofile

```
show airgroupprofile
  activate
  ccpm <name>
  domain <name>
  ipv6 <name>
  network default
  service <service-name>
  <profile-name>
```

Description

This command shows the AirGroup profile settings.

Parameter	Description
activate	Shows the active AirGroup profile.
ccpm <name>	Shows the AirGroup ClearPass Policy Manager profile.
domain <name>	Shows the AirGroup domain profile.
ipv6 <name>	Shows the AirGroup IPv6 profile.
network default Enter MAC-Address or MAC-OUI to be blacklisted/denylisted Configure max allowed IP per device. Default: 4 Configure max allowed tokens/cache per device (Default: 40) 40	Shows the default AirGroup network profile. The Enter MAC-Address or MAC-OUI to be blacklisted /denylisted lists any blacklisted /denylisted MAC address. The Configure max allowed IP per device. Default: 4 lists the maximum number of IP addresses.

Parameter	Description
	The Configure max allowed tokens/cache per device (Default: 40) lists the maximum number of cache entries.
<code>service <service-name></code>	Shows the AirGroup service profile.
<code><profile-name></code>	Shows the AirGroup profile settings ClearPass Policy Manager details. <ul style="list-style-type: none"> ■ entries: Shows information for devices registered in ClearPass Policy Manager. ■ server-group: Shows ClearPass Policy Manager server group information.

Example

The following example shows the current status of the AirGroup service default-airplay:

```
(host) [mynode] #show airgroupprofile service default-airplay

Airgroup Service Profile "default-airplay"
-----
Parameter          Value
-----
Service Id         _airplay._tcp
Service Id         _appletv-v2._tcp
Service Id         _raop._tcp
Service Description AirPlay
The following example shows the current status of the AirGroup default
network profile:
(host) [mynode] #show airgroupprofile network default
```

```

Network profile "default" (Predefined (changed))
-----
Parameter                                     Value
-----
Enter MAC-Address or MAC-OUI to be blacklisted/denylisted      N/A
Configure max allowed IP per device. Default: 4                 4
Configure max allowed tokens/cache per device (Default: 40)    40

```

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>network default</code> parameter was updated to include the following sub-parameters: <ul style="list-style-type: none"> ■ Enter MAC-Address or MAC-OUI to be blacklisted ■ Configure max allowed IP per device. Default: 4 ■ Configure max allowed tokens/cache per device (Default: 40)
ArubaOS 8.6.0.3	The <code>network default</code> parameter was introduced.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroupservice

show airgroupservice [dlna|mdns|verbose]

Description

This command shows information about AirGroup services.

Parameter	Description
dlna	Shows the DLNA services.
mdns	Shows the mDNS services.
verbose	Shows additional information of services.

Example

The following example shows the information of AirGroup DLNA services:

```
(host) [mynode] #show airgroupservice dlna

AirGroupService Table
-----
Service      status      service ID
Auto Associate Description
-----
-----
DIAL          Enabled     urn:dial-multiscreen-org:service:dial:1
              DIAL supported by Chromecast, FireTV, Roku etc
              urn:dial-multiscreen-org:device:dial:1
DLNA Media    Enabled     urn:schemas-upnp-org:device:MediaServer:1
              Media
              urn:schemas-upnp-org:device:MediaServer:2
              urn:schemas-upnp-org:device:MediaServer:3
              urn:schemas-upnp-org:device:MediaServer:4
              urn:schemas-upnp-org:device:MediaRenderer:1
              urn:schemas-upnp-org:device:MediaRenderer:2
              urn:schemas-upnp-org:device:MediaRenderer:3
              urn:schemas-upnp-org:device:MediaPlayer:1
DLNA Print    Disabled    urn:schemas-upnp-org:device:Printer:1
              Print
              urn:schemas-upnp-org:service:PrintBasic:1
              urn:schemas-upnp-org:service:PrintEnhanced:1
allowall      Enabled     urn:smartspeaker-audio:service:SpeakerGroup:1
              Remaining-Services
              urn:schemas-upnp-org:device:ZonePlayer:1
              urn:schemas-upnp-org:service:ConnectionManager:1
              urn:schemas-upnp-org:service:ContentDirectory:1
              urn:schemas-upnp-org:service:AlarmClock:1
```

```
urn:schemas-upnp-org:service:MusicServices:1
urn:schemas-upnp-org:service:DeviceProperties:1
urn:schemas-upnp-org:service:SystemProperties:1
urn:schemas-upnp-org:service:ZoneGroupTopology:1
urn:schemas-upnp-org:service:GroupManagement:1
urn:schemas-tencent-com:service:QPlay:1
urn:schemas-upnp-org:service:RenderingControl:1
urn:schemas-upnp-org:service:AVTransport:1
urn:schemas-sonos-com:service:Queue:1
urn:schemas-upnp-org:service:GroupRenderingControl:1
```

```
Num Services:4
Num Service-ID:28
```

The output of this command includes the following parameters:

Column	Description
Service	Shows the name of the AirGroup DLNA service.
status	Shows the status of the AirGroup DLNA service.
service ID	Shows the AirGroup DLNA service ID.
Description	Shows the description of the AirGroup DLNA service.

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show airtgroup	This command shows the global AirGroup settings.
show airtgroupprofile	This command shows the AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airmatch ap-partition

```
show airmatch ap-partition status detail <cluster-name>
```

Description

This command displays information about the partition of APs for cluster manager.

Syntax

Parameter	Description
status	Displays AP partition status.
detail	Displays details of AP partition.

Example

The following command displays information about the AirMatch debug data of an AP,

```
(host7) [mynode] #show airmatch ap-partition status detail
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The following output parameters were added for AP-555 access points: <ul style="list-style-type: none"> ■ AP in Tri-Radio Mode ■ AP Tri-Radio Mode Last UpdTime
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug advanced db-size

show airmatch debug advanced db-size

Description

This command displays database statistics and database collection statistics.

Examples

The example below indicates the AirMatch statistics related to the APs:

```
(host)#show airmatch debug advanced db-size

AirMatch DB Statistics
-----
Number of Collections:      24
DB size (in MB):           0

AirMatch DB Collection Statistics
-----
Collection                  Number of Documents      Storage Size (Bytes)
-----
action_proto                0                          0
amon_stat                   2                          840
ap_info                     2                          1120
ap_name                     2                          200
cli                         0                          0
client_history              5                          2000
configs                     1                          560
```

counters	1	36
db_stat	1	8000
local_time	4	576
logs	0	0
nbr_pathloss	0	0
optimization	0	0
pathloss_history	0	0
priority_rf_event	0	0
proc_pathloss	0	0
radio_feasibility	0	0
radio_history	0	0
radio_plan	0	0
reporting_radio	5	4720
rf_event	0	0
schedule	1	368
snapshot	30	79728
system.indexes	37	3736

Note: Stale documents are purged periodically.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug advanced stat

```
show airmatch debug advanced stat
  ap
  channel
  deployment
  eirp
  event
  nbr
  radio
```

Description

This command displays detailed statistics about the APs or radios on a Mobility Conductor.

Parameter	Description
ap	Statistics related to the APs
channel	Statistics related to channel and channel bandwidth assignment
deployment	Statistics related to channel and EIRP deployment
eirp	Statistics related to the EIRP assignment
event	Statistics related to RF events
nbr	Statistics related to radio neighbors
radio	Statistics related to radios

Examples

The example below indicates the AirMatch statistics related to the APs:

```
(host)#show airmatch debug advanced stat ap

Field                               Value
----                               -
Number of APs                       2304
+-----+
|Number of 5GHz Radios per AP model|
+-----+
AP Model                             Count
-----
AP-205H                              1224
AP-224                               47
AP-225                               976
```



```

AP-275                    55
AP-365                    1
+-----+
|Number of 2.4GHz Radios per AP model|
+-----+
AP Model                  Count
-----
AP-205H                  1224
AP-224                   47
AP-225                   976
AP-275                   56
AP-365                   1

```

The example below indicates the AirMatch statistics related to the radios:

```

(host)#show airmatch debug advanced stat radio
Field                      Count
-----
Radios                     4607
Active Radios              4607
Inactive Radios            0
Radios with Up-to-date Info 4607
Radios with Stale Info     0
+-----+
|5GHz Radios|
+-----+
Field                      Count
-----
Radios                     2303
Active Radios              2303
Inactive Radios            0
Active Radios with Up-to-date Info 0
+-----+
|2.4GHz Radios|
+-----+
Field                      Value
-----
Radios                     2304
Active Radios              2304
Inactive Radios            0
Active Radios with Up-to-date Info 0

```

The example below indicates the AirMatch statistics related to the channels:

```

(host)#show airmatch debug advanced stat channel

+=====+
|Channel Distribution|
+=====+
+-----+
|5GHz Channel Bandwidth Distribution|

```

Channel Bandwidth	Count
40MHz	500
80MHz	1803

Channel Range	Count
36 - 40	41
44 - 48	39
52 - 56	41
60 - 64	46
100 - 104	43
108 - 112	41
116 - 120	45
124 - 128	41
132 - 136	40
140 - 144	39
149 - 153	43
157 - 161	41
36 - 48	304
52 - 64	305
100 - 112	305
116 - 128	291
132 - 144	299
149 - 161	299

Primary Channel	Count
36	94
40	102
44	91
48	97
52	103
56	94
60	96
64	99
100	100
104	99
108	96
112	94
116	97
120	94
124	94
128	92
132	100
136	92
140	94
144	92
149	91
153	98
157	92

```

161
-----+
|2.4GHz Channel Bandwidth Distribution|
-----+
Channel Bandwidth          Count
-----
20MHz                      2304
-----+
|2.4GHz Primary Channel Distribution|
-----+
Primary Channel           Count
-----
1                          755
6                          772
11                         777
=====+
|Summary of Channel Reasons|
=====+
+-----+
|5GHz Channel Reasons|
+-----+
Channel Reason            Count
-----
AIRMATCH_INIT            252
AIRMATCH_NOISE           7
AIRMATCH_NOISE_CLEARED   3
AIRMATCH_SOLVER          2003
RADAR_CLEARED            30
RADAR_DETECTED           8
+-----+
|2.4GHz Channel Reasons|
+-----+
Channel Reason            Count
-----
AIRMATCH_INIT            556
AIRMATCH_NOISE           14
AIRMATCH_NOISE_CLEARED   54
AIRMATCH_SOLVER          1680
=====+
|Summary of Static Channels|
=====+
Band                      Count
-----
5GHz                      0
2.4GHz                    0

```

The example below indicates the AirMatch statistics related to the EIRP assignments:

```

(host)#show airmatch debug advanced stat eirp

=====+
|EIRP Distribution|
=====+
+-----+

```

|5GHz EIRP Distribution|

+-----+

EIRP (dBm)	Count
5	10
6	4
7	13
8	10
9	22
10	34
11	57
12	133
13	263
14	221
15	216
16	270
17	280
18	308
19	167
20	107
21	65
22	44
23	42
24	13
25	6
26	7
27	2
29	2
30	7

+-----+

|2.4GHz EIRP Distribution|

+-----+

EIRP (dBm)	Count
4	33
5	23
6	41
7	67
8	199
9	292
10	315
11	240
12	255
13	353
14	254
15	119
16	38
17	20
18	19
19	15
20	3
21	1
22	1
25	15
30	1

+=====+

```

|EIRP Reasons|
+=====+
+-----+
|5GHz EIRP Reasons|
+-----+
EIRP Reason                      Count
-----
AIRMATCH_INIT                    1262
AIRMATCH_SOLVER                   1041
+-----+
|2.4GHz EIRP Reasons|
+-----+
EIRP Reason                      Count
-----
AIRMATCH_INIT                    1212
AIRMATCH_SOLVER                   1092
+=====+
|Static EIRPs|
+=====+
Band                              Count
-----
5GHz                              0
2.4GHz                            0

```

The example below indicates the AirMatch statistics related to the radio neighbors:

```

(host)#show airmatch debug advanced stat nbr

+-----+
|Radio Neighbor Discovery - 5GHz|
+-----+
Field                      Count
-----
Number of Radios Reporting Neighbors    2290
Number of Interfering Neighbors         184
Average Number of Friend Neighbors*     17
Average Number of Interfering Neighbors* 0
+-----+
|Radio Neighbor Discovery - 2.4GHz|
+-----+
Field                      Count
-----
Number of Radios Reporting Neighbors    2301
Number of Interfering Neighbors         2395
Average Number of Friend Neighbors*     22
Average Number of Interfering Neighbors* 6

```

The example below indicates the AirMatch statistics related to the channel and its EIRP deployments:

```

(host)#show airmatch debug advanced stat deployment

```

```

+-----+
|Channel/EIRP Deployment - 5GHz|
+-----+
Field                               Count
-----
Radios with AirMatch deployment      2303
Radios with AirMatch deployment completed 1891
Radios with AirMatch deployment in progress 412
Radios deployed with retries         0
Radios with Solution from last optimization 428
+-----+
|Channel/EIRP Deployment - 2.4GHz|
+-----+
Field                               Count
-----
Radios with AirMatch deployment      2304
Radios with AirMatch deployment completed 1870
Radios with AirMatch deployment in progress 434
Radios deployed with retries         0
Radios with Solution from last optimization 428

```

The example below indicates the AirMatch statistics related to RF events:

```

(host)#show airmatch debug advanced stat event

+---- +-----+
|Radar Events|
+-----+
Duration                               Number of Radios
-----
1 day                                  725
7 days                                 725
+---- +-----+
|5GHz Noise Events|
+-----+
Duration                               Number of Radios
-----
1 day                                  35
7 days                                 35
+---- +-----+
|2.4GHz Noise Events|
+-----+
Duration                               Number of Radios
-----
1 day                                  26
7 days                                 26
+-----+
|Radar Prone Channels (7 days)|
+-----+
Channel                               Number of Events
-----
116                                    130
124                                    93
128                                    84

```

120	54
132	41
136	33
60	13
100	12
140	9
104	9
144	7
108	6
64	5
112	5
52	4

```

+-----+
|Radar Prone Radios (7 days)|
+-----+

```

Radio Mac	AP Model	Number of Events	AP name
a8:bd:27:cf:54:90	AP-335	12	ARUBA-AP-01
70:3a:0e:61:43:30	AP-335	11	ARUBA-AP-04
80:3a:0e:59:6f:50	AP-335	10	ARUBA-AP-21
80:3a:0e:58:d7:d0	AP-335	10	ARUBA-AP-09
80:3a:0e:5d:20:f0	AP-335	8	ARUBA-AP-30
80:3a:0e:61:aa:10	AP-335	7	ARUBA-AP-56
80:3a:0e:61:a2:30	AP-335	6	ARUBA-AP-61
a9:bd:27:cf:85:50	AP-335	6	ARUBA-AP-01
80:3a:0e:61:a5:10	AP-335	6	ARUBA-AP-37
80:3a:0e:58:cb:d0	AP-335	5	ARUBA-AP-11

```

+-----+
|5GHz Noise Prone Channels (7 days)|
+-----+

```

Channel	Number of Events
161	9
157	8
153	7
40	6
36	5
149	3
60	3
100	2
165	1
140	1
44	1
48	1

```

+-----+
|5GHz Noise Prone Radios (7 days)|
+-----+

```

Radio Mac	AP Model	Number of Events	AP name
60:3a:0e:57:df:30	AP-335	5	ARUBA-AP-89
c5:b5:ad:0c:b3:f0	AP-303H	4	ARUBA-AP-94
60:3a:0e:60:81:f0	AP-335	4	ARUBA-AP-128
60:3a:0e:5b:57:d0	AP-335	2	ARUBA-AP-08
60:3a:0e:52:8d:b0	AP-335	2	ARUBA-AP-33
60:3a:0e:70:75:d0	AP-303H	1	ARUBA-AP-109
60:3a:0e:5c:80:f0	AP-335	1	ARUBA-AP-25

```

60:3a:0e:5c:a4:10 AP-335 1 ARUBA-AP-01
c5:b5:ad:10:81:50 AP-303H 1 ARUBA-AP-30
a4:bd:27:d4:8d:90 AP-335 1 ARUBA-AP-45
+-----+
|2.4GHz Noise Prone Channels (7 days)|
+-----+
Channel                               Number of Events
-----
1                                       56
11                                      53
6                                       52
+-----+
|2.4GHz Noise Prone Radios (7 days)|
+-----+
Radio Mac          AP Model          Number of Events  AP name
-----
c3:b5:ad:0c:b6:60 AP-303H           76               ARUBA-AP-99
10:3a:0e:57:5c:20 AP-335            20               ARUBA-AP-20
10:3a:0e:5c:7a:00 AP-335            10               ARUBA-AP-06
10:3a:0e:5b:6e:00 AP-335            4                ARUBA-AP-2
10:3a:0e:5b:56:80 AP-335            3                ARUBA-AP-25
10:3a:0e:60:fa:e0 AP-335            3                ARUBA-AP-26
10:3a:0e:5c:5f:e0 AP-335            3                ARUBA-AP-21
10:3a:0e:5f:88:e0 AP-335            2                ARUBA-AP-87
c0:b5:ad:11:4b:60 AP-303H           2                ARUBA-AP-87

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug amon-stat

show airmatch debug amon-stat

Description

Display statistics for AMON messages sent from APs to the Mobility Conductor. Each AP in a Mobility Conductor deployment measures its RF environment and then sends the managed device AMON messages about the radio feasibility based on that AP's hardware capability, radio and regulatory domain, and RF neighbors. The managed device forwards these messages to the Mobility Conductor, and the Mobility Conductor adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs. Run the `show airmatch debug amon-stat` to view details about these AMON messages.

Example

```
(ALPHA-SC) [mm] (config) #show airmatch debug amon-stat
AMON statistics for 10.20.101.12
-----
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :          366263
Number of Bytes    :      417539820
Number of Messages :          366263
ID Fields Size    Msgs      Bytes      Sequence #      Lost
%
-----
42      2 1004      366263      379448468      10676      0
0
AMON statistics for 10.20.101.13
-----
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :          283644
Number of Bytes    :      323354160
Number of Messages :          283644
ID Fields Size    Msgs      Bytes      Sequence #      Lost
%
-----
42      2 1004      283644      293855184      22764      0
0
AMON statistics for 10.20.101.20
-----
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :          136022
Number of Bytes    :      155065080
Number of Messages :          136022
ID Fields Size    Msgs      Bytes      Sequence #      Lost
%
-----
```

```

-----
- ---
42      2  1004      136022      140918792      17567      0
0
AMON statistics for 182.74.254.28
-----
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :                12599
Number of Bytes    :                14362860
Number of Messages :                12599
ID  Fields  Size      Msgs      Bytes      Sequence #      Lost
%
-----
- ---
42      2  1004      12599      13052564      93      0
0

```

The output of this command includes the following parameters:

Column	Description
Last Update Time	Time the last AMON message information was sent to Mobility Conductor
Number of Packets	Total number of AMON packets sent to Mobility Conductor since the AMON process started. This counter resets when Mobility Conductor reboots.
Number of Bytes	Total number of AMON bytes sent to Mobility Conductor since the AMON process started. This counter resets when Mobility Conductor reboots.
Number of Messages	Total number of AMON packets sent to Mobility Conductor since the AMON process started. This counter resets when Mobility Conductor reboots.
ID	The ID number of the AMON message type. ArubaOS 8.0 supports AMON messages with the message ID of 42 .
Fields	Number of fields in the AMON message. AMON messages with the message ID of 42 include two fields.
Size	Total number of bytes sent for the AMON message ID.
Msgs	Total number of messages sent for that AMON message ID.
Bytes	Total number of bytes sent for that AMON message ID.
Sequence #	For Internal use only
Lost	Number of lost messages.
%	Percentage of lost messages.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug apinfo

```
show airmatch debug apinfo
  ap-name <name>
  ethmac <mac>
  radiomac <radiomac>
```

Description

This command displays information about the AirMatch debug data of an AP.

Syntax

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch debug data.
ethmac <mac>	Ethernet MAC ID of an AP for which you want to view AirMatch debug data.
radiomac <mac>	Radio MAC ID of an AP for which you want to view AirMatch debug data.

Example

The following command displays information about the AirMatch debug data of an AP,

```
(host7) [mynode] #show airmatch debug apinfo ap-name AP555-0
Field                               Value
-----                               -
AP Name                             AP555-0
AP Ethernet MAC                     80:8d:b7:c0:0b:af
Last Update                          2019-08-25_23:16:06
AP Model                             AP-555
AP IPV4 Address                       192.168.40.2
LMS IPV4 Address                     10.8.34.240
AP Deploy Hour                       N/A
Current Opmode                       TRI_RADIO
Configured Opmodes                   DUAL_BAND,DUAL_5G
Hardware Supported Opmodes           DUAL_BAND,TRI_RADIO
Feasible Opmodes                     TRI_RADIO
Feasible Opmodes Last Update         2019-08-20_10:47:50
AP supports Wake-On-LAN              Yes
AP in Green State                    No
AP Green State Last UpdTime          N/A
AP NetMask                           255.255.255.0
2.4GHz Client Count                 0
```

```

5GHz Client Count 2
AP in Tri-Radio Mode Yes
AP Tri-Radio Mode Last UpdTime 2019-08-25_23:15:15

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The following output parameters were added for AP-555 access points: <ul style="list-style-type: none"> ■ AP in Tri-Radio Mode ■ AP Tri-Radio Mode Last UpdTime
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug client-history

```

show airmatch debug client-history
  ap-name <ap-name>
  mac <mac>

```

Description

This command displays information about the airmatch client count debug data of an AP.

Syntax

Parameter	Description
ap-name <ap-name>	Name of an AP for which you want to view airmatch client count debug data.
mac <mac>	MAC ID of an AP for which you want to view airmatch client count debug data.

Example

The following command displays information about the AirMatch debug data of an AP,

```
(host7) [mynode] #show airmatch debug client-history ap-name
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The following output parameters were added for AP-555 access points: <ul style="list-style-type: none">■ AP in Tri-Radio Mode■ AP Tri-Radio Mode Last UpdTime
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug configs

```
show airmatch debug configs
```

Description

This command displays the advanced configuration settings in the AirMatch profile. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-` output modifier helps you redirect the command output.

Example

The following command displays the configuration settings.

```
(host)[mm] #show airmatch debug configs
Field                               Value
----                               -
Radar Event Period 5GHz             1440
Noise Event Period 5GHz             1440
Noise Event Period 2GHz             1440
Run Now                             0
Deploy hour of day                  5
Deploy mode                         0
EIRP offset
TimeZone string                     PST8PDT,M3.2.0,M11.1.0
Is Active Server                    1
Is RF Planning Auto                 1
Quality Threshold                   8
Solver Feas Deploy Threshold        25
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug db-dump status

show airmatch debug db-dump status

Description

This command displays information about the status of the AirMatch debug database dump.

Example

The following example indicates the status of the AirMatch debug database dump:

```
(host)#show airmatch debug db-dump status

dbdump status info
-----
Field                Value
-----
dbdump status        SUCCESS
Begin time           2018-03-19 15:58:50
End time             2018-03-19 15:58:53
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.
airmatch db-dump	This command creates a dump of the database used by AirMatch. The dump file can be exported using the <code>copy</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug db-stat

show airmatch debug db-stat

Description

This command displays information about the AirMatch DB statistics.

Example

The following example indicates the status of the AirMatch DB statistics:

```
(host)#show airmatch debug db-stat

AirMatch DB Statistics
-----
Last Update   : 2019-04-08 00:27:36
AirMatch Counters
-----
Session Fails      Last Time      Time Shift      Last Time      Msg
Decode Fails      Last Time
-----
0
AirMatch DB Collection Counters
-----
AirMatch DB Collection Counters: Inserts
-----
Collection      Total      Fails      Last Time      Dropped*
  Last Time
-----
amon_stat          0          0          0
configs            0          0          0
logs               8          0          0
nbr_pathloss       0          0          0
pathloss_history   0          0          0
proc_pathloss      0          0          0
radio_feasibility  0          0          0
radio_history      0          0          0
reporting_radio    0          0          0
rf_event           0          0          0
db_stat            0          0          0
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug feasibility

```
show airmatch debug feasibility
  ap-name <name>
  mac <mac>
```

Description

Display information about an AP's feasibility based on that AP's hardware capability, radio and regulatory domain, and radio events such as radar detection and high noise detection.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch feasibility data
mac <mac>	MAC address an AP for which you want to view AirMatch feasibility data

Example

The following example displays feasibility information for an AP-345 access point.

```
(host) [mynode] (802.11g radio profile "default") #show airmatch debug
feasibility ap-name ard4
Field                               Value
----                               -
Mac                                  c8:b5:ad:ba:eb:c0
Updated On                           2017-10-19 18:24:48
Current Opmode                       DUAL_BAND
HW Supported Opmodes                 DUAL_BAND,DUAL_5G
Configured Opmodes                   DUAL_BAND
Feasible Opmodes                     DUAL_BAND
Chan 20MHz                            36,44,48,52
Chan 40MHz
Chan 80MHz
Chan 160MHz
Bandwidth                             20MHz
Config BW range(MHz)                 20 - 160
Hardware BW range(MHz)               20 - 40
Eirp Range Chan 20MHz                 52:[12,16] 36:[12,16] 44:[12,16] 48:[12,16]
Eirp Range Chan 40MHz
Eirp Range Chan 80MHz
Eirp Range Chan 160MHz
EIRP(dBm)                             0 - 0
Config EIRP range(dBm)               12 - 16
Hardware EIRP range(dBm)             0 - 0
EIRP Offset(dB)                       0
Band                                   5GHz
Band Range                            BAND_LOWER
```

Update Reason Flex Radio Update
Last Update 2017-10-19 18:24:48
AirMatch Radio Feasibility Band 2GHz for current opmode DUAL_BAND

Field Value

Mac c8:b5:ad:ba:eb:c0
Updated On 2017-10-19 18:24:48
Current Opmode DUAL_BAND
HW Supported Opmodes DUAL_BAND,DUAL_5G
Configured Opmodes DUAL_BAND
Feasible Opmodes DUAL_BAND
Chan 20MHz 1,6,11
Chan 40MHz 1,7
Chan 80MHz
Chan 160MHz
Bandwidth 20MHz,40MHz
Config BW range(MHz) 20 - 40
Hardware BW range(MHz) 20 - 40
Eirp Range Chan 20MHz 6:[11,12] 11:[11,12] 1:[11,12]
Eirp Range Chan 40MHz 1:[11,12] 7:[11,12]
Eirp Range Chan 80MHz
Eirp Range Chan 160MHz
EIRP(dBm) 11 - 12
Config EIRP range(dBm) 11 - 12
Hardware EIRP range(dBm) 10 - 25
EIRP Offset(dB) 0
Band 2GHz
Band Range BAND_FULL
Update Reason Flex Radio Update
Last Update 2017-10-19 18:24:48
AirMatch Radio Feasibility Band 5GHz for current opmode DUAL_BAND

Field Value

Mac c8:b5:ad:ba:eb:d0
Updated On 2017-10-19 18:24:45
Current Opmode DUAL_BAND
HW Supported Opmodes DUAL_BAND,DUAL_5G
Configured Opmodes DUAL_BAND
Feasible Opmodes DUAL_BAND
Chan 20MHz 44,48
Chan 40MHz 36,44,149,157
Chan 80MHz 52,100,116,132
Chan 160MHz 36
Bandwidth 20MHz,40MHz,80MHz,160MHz,80+80MHz
Config BW range(MHz) 20 - 160
Hardware BW range(MHz) 20 - 160
Eirp Range Chan 20MHz 44:[12,16] 48:[12,16]
Eirp Range Chan 40MHz 36:[12,16] 44:[12,16] 149:[12,16] 157:[12,16]
Eirp Range Chan 80MHz 52:[12,16] 100:[12,16] 116:[12,16] 132:[12,16]
Eirp Range Chan 160MHz 36:[12,16]
EIRP(dBm) 12 - 16
Config EIRP range(dBm) 12 - 16
Hardware EIRP range(dBm) 0 - 31
EIRP Offset(dB) 0


```

Band                5GHz
Band Range          BAND_FULL
Update Reason       Flex Radio Update
Last Update         2017-10-19 18:24:45

```

```
AirMatch Radio Feasibility Band 5GHz for alternate opmode DUAL_5G
```

```

-----
Field                Value
-----
Mac                  c8:b5:ad:ba:eb:d0
Updated On           2017-10-19 18:24:45
Current Opmode       DUAL_BAND
HW Supported Opmodes DUAL_BAND,DUAL_5G
Configured Opmodes   DUAL_BAND
Feasible Opmodes     DUAL_BAND
Chan 20MHz           100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
Chan 40MHz           149,157
Chan 80MHz           100,116,132
Chan 160MHz
Bandwidth            20MHz,40MHz,80MHz,80+80MHz
Config BW range(MHz) 20 - 160
Hardware BW range(MHz) 20 - 160
Eirp Range Chan 20MHz 112:[12,16] 140:[12,16] 149:[12,16] 161:[12,16]
116:[12,16] 136:[12,16] 144:[12,16] 100:[12,16] 153:[12,16] 157:[12,16] 124:
[12,16] 128:[12,16] 132:[12,16] 104:[12,16] 108:[12,16] 120:[12,16]
Eirp Range Chan 40MHz 149:[12,16] 157:[12,16]
Eirp Range Chan 80MHz 100:[12,16] 116:[12,16] 132:[12,16]
Eirp Range Chan 160MHz
EIRP(dBm)            0 - 0
Config EIRP range(dBm) 12 - 16
Hardware EIRP range(dBm) 0 - 0
EIRP Offset(dB)      0
Band                  5GHz
Band Range           BAND_UPPER
Update Reason         Flex Radio Update
Last Update           2017-10-19 18:24:45

```

The following example displays feasibility information for an AP-555 access point,

```

(ArubaMM-VA_A2_0E_C7) [mynode] #show airmatch debug feasibility ap-name
AP555-0
AirMatch Radio Feasibility Band 5GHz for current opmode TRI_RADIO
-----
Field                Value
-----
Mac                  80:8d:b7:80:ba:f0
Updated On           2019-08-25 22:06:44
Probe Type           Soft AP
Current Opmode       TRI_RADIO
HW Supported Opmodes DUAL_BAND,TRI_RADIO
Configured Opmodes   DUAL_BAND,DUAL_5G
Feasible Opmodes     TRI_RADIO
Chan 20MHz           36,40,44,48

```

```

Chan 40MHz          36,44
Bandwidth           20MHz,40MHz
Config BW range(MHz) 20 - 40
Hardware BW range(MHz) 20 - 80
Eirp Range Chan 20MHz 36:[5,10] 40:[5,10] 44:[5,10] 48:[5,10]
Eirp Range Chan 40MHz 44:[5,10] 36:[5,10]
EIRP (dBm)         5 - 10
Config EIRP range (dBm) 5 - 10
Hardware EIRP range (dBm) 0 - 27
EIRP Offset (dB)   0
Band               5GHz
Band Range         BAND_LOWER
Update Reason      Periodic Update
Last Update        2019-08-25 22:06:44

```

Column	Description
Mac	MAC address of the AP radio
Updated On	The last time the AP radio's feasibility information was updated in the Mobility Conductor database
Current Opmode	Current operation mode
HW Supported Opmodes	Supported operation modes
Configured Opmodes	Configured operation modes
Feasible Opmodes	Feasible operation modes
Chan 20MHz	List of feasible channels in 20 MHz bandwidth
Chan 40MHz	List of feasible channels in 40 MHz bandwidth
Chan 80MHz	List of feasible channels in 80 MHz bandwidth
Chan 160MHz	List of feasible channels in 160 MHz bandwidth
Bandwidth	List of feasible channel bandwidths
Config BW range(MHz)	List of configured channel bandwidths
Hardware BW range(MHz)	List of channel bandwidths supported by the hardware
Eirp Range Chan 20MHz	Range of EIRPs supported for each channel in a 20 MHz channel bandwidth
Eirp Range Chan 40MHz	Range of EIRPs supported for each channel in a 40 MHz channel bandwidth

Column	Description
Eirp Range Chan 80MHz	Range of EIRPs supported for each channel in a 80 MHz channel bandwidth
Eirp Range Chan 160MHz	Range of EIRPs supported for each channel in a 160 MHz channel bandwidth
EIRP (dBm)	Current supported EIRP range, in dBm.
Config EIRP range (dBm)	Configurable EIRP range, in dBm
Hardware EIRP range (dBm)	Hardware EIRP range, in dBm
EIRP Offset (dB)	Offset of the EIRP added to the computed EIRP (in dB)
Band	Operational Band, in GHz
Band Range	Current band range
Update Reason	Reason for previous feasibility update, such as a periodic update, radar detection, changes to a regulatory domain profile, or a radio band change for an AP radio that can operate in flex-radio mode. An AP radio that supports flex mode can operate as a single radio in the 2.4 GHz band, a single radio in the 5 GHz band, or as two radios, operating separately in the 2.4 GHz and 5 GHz bands.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output will display the tri-radio mode values for AP-555 access points.
ArubaOS 8.3.0.0	The following parameters were introduced in the command output:

Release	Modification
	<ul style="list-style-type: none"> ■ Current Opmode ■ HW Supported Opmodes ■ Configured Opmodes ■ Feasible Opmodes ■ Eirp Range Chan 20MHz ■ Eirp Range Chan 40MHz ■ Eirp Range Chan 80MHz ■ Eirp Range Chan 160MHz
ArubaOS 8.2.0.0	The output in the EIRP field can display EIRP values in .1 dBm increments, and the Update Reason field can show if an AirMatch update was made due to a radio band change by an AP radio that supports both 1x1 dual radio mode and 2x2 single radio mode.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug history

```
show airmatch debug history
  ap-name <name>
  mac <mac>
```

Description

This command displays a history of AirMatch updates to an AP radio's channel, bandwidth, EIRP or mode.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch history data
mac <mac>	MAC address of an AP's radio (BSSID address) for which you want to view AirMatch history data

Example

```
(host)[mm] #show airmatch debug history ap-name West-2-155
2GHz      radio mac 6c:f3:7f:78:e2:80  ap name West-2-155
-----
Time of Change      Chan      Bandwidth  EIRP (dBm)  Mode      Source
-----
2016-06-07 05:34:45  11-> 1    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-06-06 05:34:24  1-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-06-05 05:35:00  6-> 1     20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-06-04 05:34:55  11-> 6    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-06-02 05:34:30  6-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-06-01 05:34:48  11-> 6    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-30 05:32:44  6-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-29 05:35:41  11-> 6    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-28 05:34:49  1-> 6     20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-27 05:34:29  11-> 1    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-26 05:34:33  6-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-25 05:34:27  11-> 6    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-24 05:34:51  6-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-22 05:32:01  1-> 6     20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-21 05:31:40  11-> 1    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-19 05:32:51  11-> 1    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-18 05:34:02  1-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-17 05:33:57  6-> 1     20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-14 05:34:17  11-> 6    20-> 20     9.0-> 9.0   AP ->AP    Solver
2016-05-13 05:34:27  1-> 11    20-> 20     9.0-> 9.0   AP ->AP    Solver

5GHz      radio mac 6c:f3:7f:78:e2:90  ap name West-2-155
-----
Time of Change      Chan      Bandwidth  EIRP (dBm)  Mode      Source
```

```

-----
2016-06-07 05:33:45 40->149 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-06-06 05:33:24 44-> 40 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-06-05 05:34:00 52-> 44 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-06-03 05:33:27 161-> 52 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-06-02 05:33:30 40->161 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-31 05:33:25 153-> 40 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-30 05:31:44 44->153 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-29 05:34:41 40-> 44 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-28 05:33:49 60-> 36 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-27 05:33:29 64-> 60 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-26 05:33:33 149-> 64 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-25 05:33:27 56->149 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-24 05:33:50 48-> 56 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-23 05:32:50 36-> 48 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-22 05:31:01 52-> 36 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-21 05:30:40 40-> 52 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-20 05:35:40 40-> 60 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-19 05:31:50 40-> 52 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-18 05:33:02 161-> 40 40-> 40 18.0-> 18.0 AP ->AP Solver
2016-05-17 05:32:57 56->161 40-> 40 18.0-> 18.0 AP ->AP Solver

```

The output of this command includes the following parameters:

Column	Description
Time of Change	Timestamp showing when the change was made.
Chan	Previous and current channel assignments .
Bandwidth	Previous and current bandwidth assignments.
EIRP (dBm)	Previous and current EIRP levels.
Mode	Previous and current AP mode. Supported modes are AP and APM (Air Monitor).
Source	Source of the confirmation changes. AP changes made as a result of AirMatch calculations appear with the source type of "solver".

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output in the EIRP field can display EIRP values in .1 dBm increments.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug nbr

```
show airmatch debug nbr
  ap-name <name>
  mac <mac>
```

Description

This command displays information about neighbor APs seen by an AP that is managed over AirMatch.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch neighbor data.
mac <mac>	MAC address an AP for which you want to view AirMatch neighbor data.

Example

```
(host) [mm] #show airmatch debug nbr ap-name ssa-155A
2GHz radio mac 6c:f3:7f:78:e3:80 ap name ssa-155
-----
-----
Nbr Mac          Is Friend  Path Loss (dB)  Channel  Last Update
AP Name
-----
-----
c4:e9:84:67:d4:c0          49          1    2016-06-08 01:50:16
00:1a:8c:9f:56:a8          65          11   2016-06-07 23:15:43
00:1a:8c:9f:56:b8          71          6    2016-06-08 00:48:00
be:d1:d3:91:87:c8          82          6    2016-06-07 12:57:51
a2:f8:95:b1:a5:10          83          11   2016-06-06 20:56:47
00:1a:8c:9f:56:c8          85          1    2016-06-08 01:50:16
e0:98:61:a6:77:c0          85          1    2016-06-06 17:00:55
00:1a:8c:9f:56:70          86          13   2016-06-08 01:50:17
70:5a:9e:a6:19:50          86          11   2016-06-08 00:16:52
c4:e9:84:67:da:68          87          4    2016-06-08 01:50:17
8a:dc:96:1e:10:f8          87          6    2016-06-08 01:19:19
```

The following output displays the output for AP-555 access point,

```
(host) [mynode] #show airmatch debug nbr ap-name AP555-0
5GHz radio mac 80:8d:b7:80:ba:f0 ap name AP555-0
-----
-----
```


Nbr Mac Update	Is Friend	Pathloss (db)	Channel	Bandwidth	Flag	Last	AP Name
f0:5c:19:1f:28:d0 09-10_	*	36	44	CBW_UNKNOWN	NR	2019-	
23:15:14 c8:b5:ad:ba:f8:f0 09-10_	*	39	153	CBW40	R	2019-	
23:15:15 90:4c:81:73:82:10 09-10_	*	42	44	CBW40	NR	2019-	AP345
23:15:14 80:8d:b7:81:07:c0 09-10_	*	52	149	CBW_UNKNOWN	NR	2019-	
23:15:12 80:8d:b7:80:b7:90 09-10_	*	62	48	CBW40	NR	2019-	
23:15:14 80:8d:b7:80:b7:80 09-10_	*	62	157	CBW80	NR	2019-	

The output of this command includes the following parameters:

Column	Description
Nbr Mac	MAC address of the neighbor AP.
Is Friend	Indicates whether the neighbor AP is associated to the same Mobility Conductor as the reporting AP.
Path Loss (dB)	Path loss between the neighbor AP and reporting AP, in dB.
Channel	Radio channel used by the neighbor AP.
Last Update	Date and time the reporting AP last received updated information from the neighbor AP.
AP Name	Name of the neighbor AP. The AP name will only appear if the neighbor AP is managed by the same Mobility Conductor as the reporting AP.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output for AP-555 access points will display information about Radio 2 which is the upper 5Ghz radio.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug optimization

```
show airmatch debug optimization
  advanced partition
  [last | <seq>]
  [sort-by {ap-name | band | bandwidth | channel | eirp | rf-domain-id}]
  [descending]
```

Description

This command displays a list of RF debug optimizations performed by AirMatch.

Parameter	Description
advanced partition	Advanced partition information.
last	Last debug optimization.
<seq>	Optimization sequence number.
sort-by	Sorts the results in ascending order and on a per-band basis. Use this after specifying an optimization number or last as the value.
ap-name	Sorts results based on the AP name. Ascending order
band	Sorts results based on the band. 2 GHz, 5 GHz Ascending order
bandwidth	Sorts results based on the bandwidth. Ascending order
channel	Sorts results based on the channel. Ascending order
eirp	Sorts results based on the EIRP. Ascending order
rf-domain-id	Sorts results based on the RF domain ID. Ascending order
descending	Sort results in descending order.

Example

The following example shows a detailed summary of the RF debug optimization:

```
(host) [mm] #show airmatch debug optimization
```

Seq	Time	APs	[5GHz] Radios	Cost	Conflict
#13	2018-03-23_02:45:07	3	3	4	0
#12	2018-03-22_05:35:58	3	3	4	0
#11	2018-03-21_10:15:55	3	3	4	0
#10	2018-03-21_09:17:14	3	3	2	0
#9	2018-03-20_12:00:51	3	3	2	0
#8	2018-03-19_12:00:47	3	3	2	0
#7	2018-03-18_12:00:46	3	3	2	0
#6	2018-03-17_12:00:43	3	3	2	0
#5	2018-03-16_12:00:40	3	3	2	0
#4	2018-03-15_12:00:39	3	3	2	0
#3	2018-03-14_12:00:42	3	3	2	0
#2	2018-03-14_08:10:32	3	3	2	0
#1	2018-03-14_05:54:50	1	1	2	0

[2GHz] Radios	Cost	Conflict	Type	Computed	Computed
3	4	0	On-demand	Yes	No
3	4	0	On-demand	Yes	No
3	4	0	On-demand	Yes	No
3	4	0	On-demand	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	No
3	4	0	Scheduled	Yes	Yes
3	4	0	On-demand	Yes	No
1	4	0	On-demand	Yes	No

* EIRP is always computed in optimization

The following example shows a detailed summary of the RF debug optimization for a given sequence number:

```
(host) [mynode] #show airmatch debug optimization 77
# Seq #77 2020-10-22_15:50:52 Opmode
# 5GHz network cost/solution cost: 4.9/5
# 2.4GHz network cost/solution cost: 13/11.3
# Opmode Computed: true
# Opmode Deployed: true
# Band Radio RFDom Part Chan CBW EIRP(dBm) Opmode
Opmode Client Band APName
ID ID Reason Pref Pref
```

```

-----
-----
2GHz d0:d3:e0:b2:e8:a0 001 000 6 20 10.0t DUAL_BAND
S a F AP56x
2GHz 20:a6:cd:34:bd:60 001 000 6 20 10.0t DUAL_BAND
S a F AP325-Airmonitor
2GHz 70:3a:0e:96:60:00 001 000 1 20 10.0t DUAL_BAND
S a F AP315-Airmonitor
2GHz 80:8d:b7:81:07:e0 001 000 1 20 10.0t DUAL_BAND
C1 a F
2GHz 9c:8c:d8:76:10:30 001 000 6 20 10.0t DUAL_BAND
C1 a F AP555-2
2GHz 80:8d:b7:80:f8:b0 001 000 1 20 10.0t DUAL_BAND
C1 a F AP555-new
2GHz 38:17:c3:8f:87:60 001 000 11 20 10.0t DUAL_BAND
S a F AP344-1
2GHz d0:15:a6:75:69:c0 001 000 11 20 10.0t DUAL_BAND
S a F AP505H
2GHz 38:17:c3:8b:a3:e0 001 000 11 20 10.0t DUAL_BAND
S a F AP344-2
5GHz 38:17:c3:8b:a3:f0 001 000 36 20 11.0t DUAL_BAND
S A F AP344-2
5GHz 80:8d:b7:81:07:d0 001 000 165 20 11.0t DUAL_BAND
C1 p F
5GHz 20:a6:cd:34:bd:70 001 000 48 20 11.0t DUAL_BAND
S A F AP325-Airmonitor
5GHz d0:d3:e0:b2:e8:b0 001 000 153 20 11.0t DUAL_BAND
S p F AP56x
5GHz d0:15:a6:75:69:d0 001 000 40 20 11.0t DUAL_BAND
S A F AP505H
5GHz c8:b5:ad:ba:f8:f0 001 000 161 20 10.0t DUAL_5G
S A F AP345-1-desk
5GHz 38:17:c3:8f:87:70 001 000 36 20 11.0 DUAL_BAND
S A F AP344-1
5GHz 9c:8c:d8:76:10:20 001 000 161 20 11.0 DUAL_BAND
C1 A F AP555-2
5GHz 70:3a:0e:96:60:10 001 000 157 20 11.0t DUAL_BAND
S A F AP315-Airmonitor
5GHz c8:b5:ad:ba:f8:e0 001 000 44 20 15.0t DUAL_5G
S A F AP345-1-desk
5GHz 80:8d:b7:80:f8:a0 001 000 149 20 11.0t DUAL_BAND
C1 p F AP555-new
[*] regarded frozen | [i] channel ignored because insufficient quality
increase | [t] EIRP truncated
Opmode Reason - S : Singleton | Cp : Capacity | C1 : Coverage I | C2
: Coverage II | C3 : Coverage III | U : Unknown
Client Preference - [p] HE Preferred | [n] Non-HE Preferred | [a] Allow-
All | [A] Allow-All AirMatch Assigned
Band Preference - [L] 5GHz-Lower | [U] 5GHz-Upper | [F] 5GHz-Full

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.8.0.0	A new flag, A was introduced to indicate the radios assigned by AirMatch.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug pathloss history rep-radio

```
show airmatch debug pathloss history rep-radio
  ap-name <name>
  nbr-radio
    nbr-ap-name
    nbr-bssid
  bssid <radio-bssid>
```

Description

This command displays information about the recent AirMatch debug path loss.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch debug path loss history.
nbr-radio	Specify one of the following neighbor radio details: <ul style="list-style-type: none">▪ nbr-ap-name <nbr-ap-name>: Specify neighbor AP name.▪ nbr-bssid <nbr-bssid>: Specify neighbor radio BSS ID.
bssid <radio-bssid>	Shows the debug path loss history for a specific BSSID.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug populate-db

```
show airmatch debug populate-db
  status
    all
    ap-info
    feasibility
```

Description

This command displays information about the database population of the collection.

Syntax

Parameter	Description
status	Displays database population status information.
all	Displays status of all required collections in database.
ap-info	Displays status of ap-info collection population.
feasibility	Displays status of feasibility collection population.

Example

The following command displays information about the AirMatch debug data of an AP,

```
(host7) [mynode] #show airmatch debug populate-db status
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airmatch debug reporting-radio

```
show airmatch debug reporting-radio
  ap-name <name>
  mac <mac>
  list-all
```

Description

Displays details for an AP radio reporting AirMatch data to a Mobility Conductor.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch radio data.
mac <mac>	MAC address an AP for which you want to view AirMatch radio data.
list-all	Lists all the radios in the database.

Example

```
(host) [mm] #show airmatch debug reporting-radio ap-name ssa-155
Field                Value
-----
Band                 5GHz
AP Ethernet MAC      9c:1c:12:c0:86:c6
Radio MAC            9c:1c:12:88:6c:70
AP Name              ard4
AP Model             AP-225
LMS IP               10.3.22.222
Last Update          2016-10-24 17:04:44
Channel              161
Bandwidth            40MHz
Channel Reason       AirMatch - Solver
Channel Update Time  2016-10-22 05:04:52
EIRP                 12.0 (dBm)
EIRP Reason          AirMatch - Init
EIRP Update Time     2016-10-12 13:29:03
Is Active            true
Is Static Chan       false
Is Static EIRP       false
Is Static CSR        false
```

Following is the output for AP-555 access points,

```
(host) [mynode] #show airmatch debug reporting-radio ap-name AP555-0
```

```

Field          Value
-----
Band           5GHz
AP Ethernet MAC 80:8d:b7:c0:0b:af
Radio MAC      80:8d:b7:80:ba:f0
AP Name        AP555-0
AP Model       AP-555
Switch IP      10.8.34.240
Last Update    2019-09-10 23:47:45
Channel        161
Bandwidth      40MHz
Channel Reason  Random
Channel Update Time 2019-09-10 23:09:42
EIRP           7.5 (dBm)
EIRP Reason    AirMatch - Min EIRP Change
EIRP Update Time 2019-09-10 23:47:45
Is Active      true
Is Static Chan false
Is Static EIRP false
Is Static CSR  false
Deploy Hour    N/A
Retries        0
Last Retry Time N/A
Local Time     PST8PDT,M3.2.0,M11.1.0
5GHz Client count 0
5GHz Count UpdTime 2019-09-10 23:40:01

```

The following example displays the output using the list-all parameter:

```

(host) [mynode] #show airmatch debug reporting-radio list-allRadios found
on Database : 27
Radios Display Limit : 20000
Static Static Radio Client
Radio Base Mac Last Update Time Band Chan EIRP Channel/ BW /EIRP
Num Pref AP Name
-----
-----
20:a6:cd:34:bd:60 2020-11-20 11:34:04 2GHz No No 1/ 20/ 10.0
1 A AP325-Airmonitor
20:a6:cd:34:bd:70 2020-11-20 11:33:53 5GHz No No 157/ 20/ 15.0
0 A AP325-Airmonitor
38:17:c3:8b:a3:e0 2020-11-20 11:28:27 2GHz No No 11/ 20/ 10.0
1 A AP344-2
38:17:c3:8b:a3:f0 2020-11-20 11:25:40 5GHz No No 149/ 20/ 12.0
0 A AP344-2
38:17:c3:8f:87:60 2020-11-20 11:28:59 2GHz No No 11/ 20/ 10.0
1 A AP344-1
38:17:c3:8f:87:70 2020-11-20 11:32:00 5GHz No No 149/ 20/ 12.0
0 A AP344-1
70:3a:0e:96:60:00 2020-11-20 11:33:38 2GHz No No 1/ 20/ 10.0
1 A AP315-Airmonitor
Client Preference - [p] HE Preferred | [n] Non-HE Preferred | [a] Allow
All | [A] Allow-All AirMatch Assigned

```

The output of this command includes the following parameters:

Column	Description
Band	Radio band used by the AP
AP Ethernet MAC	MAC address of the Ethernet interface
Radio MAC	MAC address of the AP radio
AP Name	Name of the AP
AP Model	AP model type
LMS IP	IP address of the controller to which the AP is associated
Last Update	Timestamp showing the date and time the AP last sent an update to Mobility Conductor
Channel	Channel used by the AP radio
Bandwidth	Bandwidth used by the AP radio
Channel Reason	Reason why the channel was modified
Channel Update Time	Timestamp showing the date and time that the channel was updated
EIRP	Radio EIRP, in dBm.
EIRP Reason	Reason why the EIRP setting was modified
EIRP Update Time	Timestamp showing the date and time that the EIRP setting was updated
Is Active	Indicates if the AP is active on the network.
Is Static Chan	Indicates if the AP has been assigned to a static channel
Is Static EIRP	Indicates if the AP has been assigned to a static EIRP level
Is Static CSR	Indicates if the AP has been assigned to a static Cell Size Reduction (CSR) value. Cell Size Reduction settings control Rx sensitivity for the AP. When it is set to a specific value, the radio will not receive any frames with SNR/RSSI below this configured value.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.8.0.0	A new flag, A was introduced to indicate the radios assigned by AirMatch.
ArubaOS 8.6.0.0	The output for AP-555 access points will display 5GHz Client count .
ArubaOS 8.2.0.0	The output in the EIRP field can display EIRP values in .1 dBm increments.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug schedule

```
show airmatch debug schedule
  job-list
  switch-info
```

Description

This command displays details about deployment schedules when AirMatch updates are sent to the APs.

Parameter	Description
job-list	The scheduled deployment time and duration details of APs as per the timezone.
switch-info	The timezone and deploy configured on the switch.

Example

```
(host) [mynode] #show airmatch debug schedule switch-info

# Generated: 2020-05-16_22:56:44   MM deploy time: 5:00   MM time zone: IST-5:30
# Switch IP                        Time zone
-----
-----
      <-08>8                        1.6.2.221
      <-08>8                        220.227.73.89
      <-08>8                        10.20.101.36
PST8PDT,M3.2.0,M11.1.0             11:12:11:11::2
      IST-5:30                      10.20.101.20
      IST-5:30                      10.20.101.7
      IST-5:30                      10.20.101.12
      IST-5:30                      2001:1001::201
      IST-5:30                      10.20.101.8
PST8PDT,M3.2.0,M11.1.0
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output of the <code>show airmatch debug schedule switch-info</code> command was modified to include IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug solution

```
show airmatch debug solution
  ap-name
  list-all
  mac
  switch-ip
```

Description

This command displays information about the current solution.

Syntax

Parameter	Description
ap-name <ap-name>	Displays information about the specific AP in the configuration.
list-all	Displays all radios in the database.
mac <mac>	Displays information about specific radio base MAC.
switch-ip <switch-ip>	Displays information about specific switch.

Example

```
(host7) [mynode] #show airmatch debug solution list-all

# Band Radio          Chan/Opt#    CBW      EIRP(dBm)/Opt# Client Band
Chan Time            EIRP Time   Confirm Time      Retries APName
                    Pref      Pref
-----
-
No active radios found
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airmatch debug solver feasibility

```
show airmatch debug solver feasibility
  optimization <seq> {ap-name <ap-name> | bssid <bssid>}
```

Description

Displays the feasibility information used by AirMatch Solver for a particular AP or MAC address during optimization. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
optimization	Displays the optimization history.
<seq>	Specify a sequence number to view details for a specific AirMatch solution.
ap-name <name>	Specify the name of an AP with the <ap-name> parameter to view AirMatch solver for the radios on that AP.
bssid <bssid>	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.

Example

```
(host) [mm] #show airmatch debug solver feasibility optimization 284 ap-name
AP345_DEV4
Field                               Value
-----                               -
Mac                                  c8:b5:ad:ba:bc:40
AP Name                              AP345_DEV4
Band                                  5GHz
Optimization ID                      284
Computed On                          2018-02-26_04:45:31
Chan 20MHz                            36,40,44,48
Chan 40MHz                             36,44
Chan 80MHz                             36
Chan 160MHz                            36
Bandwidth                             20MHz,40MHz,80MHz

Field                               Value
-----                               -
Mac                                  c8:b5:ad:ba:bc:50
AP Name                              AP345_DEV4
Band                                  5GHz
Optimization ID                      284
Computed On                          2018-02-26_04:45:31
```

```

Chan 20MHz          149,153,157,161,165
Chan 40MHz          149,157
Chan 80MHz          149
Chan 160MHz
Bandwidth           20MHz,40MHz,80MHz
Field               Value
-----
Mac                 9c:8c:d8:75:fe:20
AP Name             AP555-1
Band                5GHz
Optimization ID     139
Computed On         2020-11-14_21:45:37
Chan 20MHz          36,40,44,48,149,153,157,161,165
Chan 40MHz          36,44,149,157
Chan 80MHz          36,149
Chan 160MHz
Bandwidth           20MHz,40MHz,80MHz
HE Pooling Chan Feas 36

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.8.0.0	A new output parameter, <code>HE Pooling Chan Feas</code> was introduced to display the number of HE pooling channels.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch debug static-radios

```
show airmatch debug static-radios
band 2ghz|5ghz|6ghz
```

Description

Shows AirMatch data for AP radios that have been assigned static settings.

Parameter	Description
band	Radio band for which want to view static radio data.
2 ghz	View data for 2Ghz static radios.
5 ghz	View data for 5Ghz static radios.
6 ghz	View data for 6Ghz static radios.

Example

```
(host) *[mynode] (802.11g radio profile "default") #show airmatch debug
static-radios
Static Radios for Band 5GHz
Radio Base Mac      Chan EIRP Oper   /BW   /EIRP Static /BW   Flag Last
Update Time      AP Name
Channel           Channel
-----
-----
84:d4:7e:d2:10:90 Yes  Yes    36/  160/   5    36/  160   2016-10-24
17:06:30 ap315-1
18:64:72:7e:4d:90 Yes  Yes    149/  20/   5    149/  20   2016-10-24
17:04:47 x4p3
Flag column indicates '*' if Operating Channel is different from Static
Channel configured
Note: Operating Channel can be different from Static Channel during Radar
event
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .

Command	Description
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch event

```
show airmatch event [{all-events|noise|radar|priority-events} [all-aps | ap-name  
<ap-name> | bssid <bssid>]] <yyyy-mm-dd>
```

Description

Displays radar and noise event information for a specific AP or all APs. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
all-events noise priority-events radar	Display one of the following event information of the APs in the database: <ul style="list-style-type: none">▪ all-events: Radar and Noise events in the database (sorted by latest).▪ noise: Noise event list.▪ priority-events: All priority rf-events in database.▪ radar: Radar event list.
all-aps	Display list of all the APs in the database.
ap-name <ap-name>	Specify the name of an AP to display its radar and noise events.
bssid <bssid>	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
<yyyy-mm-dd>	Show date in YYYY-MM-DD format.

Example

The following example displays the noise and radar event information for all APs in the database.

```
(host) [mynode] #show airmatch event all-events all-aps
```

Band	Event	Type	Radio	Timestamp	Chan	CBW
5GHz	RADAR_DETECT		c8:b5:ad:ba:eb:c0	2018-02-14_18:06:17	52	80MHz 345
5GHz	RADAR_DETECT		c8:b5:ad:ba:eb:d0	2018-02-13_10:35:55	140	80MHz 345

```

5GHz RADAR_DETECT c8:b5:ad:ba:eb:d0 2018-02-13_05:59:46 140 80MHz 345
5GHz RADAR_DETECT 9c:1c:12:88:6a:90 2018-02-10_04:06:02 100 80MHz 225
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-09_16:17:35 11 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-09_16:17:34 6 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-08_15:00:39 11 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-08_13:53:13 1 40MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:48:21 1 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:48:20 6 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:10:47 11 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:10:44 1 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_13:18:31 11 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_13:18:30 6 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-06_14:29:50 1 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-06_14:29:48 6 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_14:02:46 11 20MHz 345
5GHz RADAR_DETECT 9c:1c:12:88:6a:90 2018-02-05_11:57:42 52 80MHz 225
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_01:51:37 1 20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_01:51:34 11 20MHz 345
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-05_00:27:21 6 20MHz 275
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-04_23:53:55 11 20MHz 275
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-04_23:09:19 1 20MHz 275

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output will display information about Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airgroup internal-state statistics

```
show airgroup internal-state statistics [dlna|mdns|ppm|verbose]
```

Description

This command shows the statistics of packets sent and received per second by AirGroup.

Parameter	Description
dlna	Shows the DLNA statistics.
mdns	Shows the mDNS statistics.
ppm	Shows the packet per minute statistics.
verbose	Shows the detailed statistics.

Example

The following example displays the packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics

Time: Tue Jul 12 13:18:24 2016
MDNS Messages
-----
Opcode Name                               Sent Since Last Read  Sent Total  Recv
Since Last Read  Recv Total
-----  ----  -----  -----  -----
7       app                               0                               5           0
-       SDN                               0                               11090       0
Rx      Request                               N/A                             N/A         0
Rx      Response                               N/A                             N/A         0
Tx      Request-Refresh                          0                               10104       N/A
Tx      Request-discovery                        0                               1836        N/A
Tx      Request-wildcard                          0                               0           N/A
Tx      Response-Solicited                        0                               0           N/A
Tx      Response-Solicited-Fragment              0                               0           N/A
```

Tx	Response-Unsolicited	0	0	N/A
	N/A			
Tx/Rx	Total	0	0	N/A
	N/A			

DLNA Messages

Opcode	Name	Sent	Since Last Read	Sent Total	Recv	Since Last
Read	Recv Total					
-	SDN	0		365947	0	
	966861					
Rx	Query	N/A		N/A	0	
	837484					
Rx	Notify Announce	N/A		N/A	0	
	69450					
Rx	Notify Bye	N/A		N/A	0	
	6					
Tx	Response	0		33958	N/A	
	N/A					

Internal MDNS Statistics

Functionality	Hit Count	Since Last Read	Hit Count Total
Response - Cache Update	0		3176
Response	0		556
Query - prepare records + Policy	0		591
Query - Policy	0		12
Query - resp pkt gen & send	0		0
Query - Response packet send	0		331139
Query	0		591
Multicast Response propagate	0		0

Internal DLNA Statistics

Functionality	Hit Count	Since Last Read	Hit Count Total
Response - Cache Update	0		73921
Response	0		0
Query - prepare records + Policy	0		14227
Query - Policy	0		34360
Query - resp pkt gen & send	0		14170
Query - Response packet send	0		74397
Query	0		837484

MDNS Multi-controller Cluster Messages

Type	Sent	Since Last Read	Sent Total	Recv
Since Last Read	Recv Total			
Unicast Response with tag	0		0	0
0				

```

Request with tag          0          0          0
      0
Raw Response              0          0          0
      0
Multicast Propagate Raw Response 0          0          0
      0

```

DLNA Multi-controller Cluster Messages

```

-----
Type                Sent Since Last Read  Sent Total  Recv Since Last Read
Recv Total
-----
Request with tag    0                0            0                0
Raw Response        0                0            0                0

```

Packet Arrival Statistics (per minute)

```

-----
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
-----
454                      Jul 05 10:34:42   5            16

```

Cache Bucket Size

```

-----
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-----
MDNS     0                0                0                1
SSDP     0                0                0                4

```

Internal mDNS and DLNA Thread Statistics

```

-----
# Thread ID  Query since Last Read  Queries Recv Total  Queries in Queue
Peak Queries in Queue
-----
1 3368556288 0                488871            0
6
2 3343378176 0                92304             0
10
3 3318200064 0                74141             0
2
4 3293021952 0                109923            0
11
5 3267843840 0                72836             0
2

```

mDNS CPU and Throttling details

```

-----
Current CPU Utilization (%)  Throttling State  Description  Query
Pkt Dropped  Resp Pkt Dropped
-----
0.04(3)                MDNS_NO_THROTTLING  No packets dropped  0
      0

```

list of controllers in same vlan

```
-----  
Controller MAC  
-----
```

```
00:1a:1e:01:ae:28  
00:0b:86:b5:15:97  
00:1a:1e:01:99:e0  
00:0b:86:9a:4a:37  
00:0c:29:d7:6d:e3  
00:1a:1e:01:bf:70  
00:1a:1e:02:07:b0  
00:0b:86:9a:4e:77  
00:0c:29:10:8c:b8  
00:0b:86:b8:e1:d8  
00:1a:1e:01:bd:b0
```

```
list of local controllers with AirGroup devices  
-----
```

```
Controller MAC  
-----
```

```
00:0b:86:9a:4a:37  
00:0c:29:d7:6d:e3  
00:1a:1e:01:bd:b0
```

```
AirGroup users 13, AirGroup servers 5. Total devices 38
```

The following example displays the DLNA packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics dlna
```

```
Time: Tue Jul 12 13:24:01 2016
```

```
DLNA Messages  
-----
```

Opcode	Name	Sent	Since Last Read	Sent Total	Recv	Since Last
Read	Recv	Total				
-	SDN	149		366096	396	
	967257					
Rx	Query	N/A		N/A	378	
	837862					
Rx	Notify Announce	N/A		N/A	10	
	69460					
Rx	Notify Bye	N/A		N/A	0	
	6					
Tx	Response	0		33958	N/A	
	N/A					

```
Internal DLNA Statistics  
-----
```

Functionality	Hit Count	Since Last Read	Hit Count	Total
Response - Cache Update	10		73931	
Response	0		0	

```

Query - prepare records + Policy 0 14227
Query - Policy 0 34360
Query - resp pkt gen & send 0 14170
Query - Response packet send 10 74407
Query 378 837862

DLNA Multi-controller Cluster Messages
-----
Type Sent Since Last Read Sent Total Recv Since Last Read
Recv Total
-----
Request with tag 0 0 0
Raw Response 0 0 0

Packet Arrival Statistics (per minute)
-----
Peak Packet Arrival Rate Peak Arrival Time No. Servers No. Clients
-----
454 Jul 05 10:34:42 5 16

Cache Bucket Size
-----
Service AP Name Bucket AP FQLN Bucket User Name Bucket Default Bucket
-----
SSDP 0 0 0 4

Internal DLNA Thread Statistics
-----
# Thread ID Query since Last Read Queries Recv Total Queries in Queue
Peak Queries in Queue
-----
1 3368556288 180 489051 0
6
2 3343378176 60 92216 0
10
3 3318200064 36 73770 0
2
4 3293021952 54 109965 0
11
5 3267843840 48 72860 0
2

MDNS CPU and Throttling details
-----
Current CPU Utilization (%) Throttling State Description Query
Pkt Dropped Resp Pkt Dropped
-----
0.03(3) MDNS_NO_THROTTLING No packets dropped 0
0

```

The following example displays the mDNS packets sent and received per second by AirGroup:

(host) [mynode] #show airgroup internal-state statistics mdns

Time: Tue Jul 12 13:26:03 2016

MDNS Messages

Opcode	Name	Since Last Read	Recv Total	Sent Since Last Read	Sent Total	Recv
7	app		0	0	5	0
-	SDN		4152	2	11092	0
Rx	Request		591	N/A	N/A	0
Rx	Response		556	N/A	N/A	0
Tx	Request-Refresh		N/A	2	10106	N/A
Tx	Request-discovery		N/A	0	1836	N/A
Tx	Request-wildcard		N/A	0	0	N/A
Tx	Response-Solicited		N/A	0	0	N/A
Tx	Response-Solicited-Fragment		N/A	0	0	N/A
Tx	Response-Unsolicited		N/A	0	0	N/A
Tx/Rx	Total		N/A	2	0	N/A

Internal MDNS Statistics

Functionality	Hit Count Since Last Read	Hit Count Total
Response - Cache Update	0	3176
Response	0	556
Query - prepare records + Policy	0	591
Query - Policy	0	12
Query - resp pkt gen & send	0	0
Query - Response packet send	232	331371
Query	0	591
Multicast Response propagate	0	0

MDNS Multi-controller Cluster Messages

Type	Since Last Read	Recv Total	Sent Since Last Read	Sent Total	Recv
Unicast Response with tag			0	0	0
Request with tag			0	0	0

```

Raw Response                                0                0                0
      0
Multicast Propagate Raw Response 0                0                0
      0

Packet Arrival Statistics (per minute)
-----
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
-----
454                        Jul 05 10:34:42    5             16

Cache Bucket Size
-----
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-----
MDNS      0                0                0                1

Internal MDNS Thread Statistics
-----
#  Thread ID  Query since Last Read  Queries Recv Total  Queries in Queue
Peak Queries in Queue
-  - - - - -  - - - - -  - - - - -  - - - - -
-----
1  3368556288  0                0                0
6
2  3343378176  0                148              0
10
3  3318200064  0                407              0
2
4  3293021952  0                12               0
11
5  3267843840  0                24               0
2

MDNS CPU and Throttling details
-----
Current CPU Utilization (%)  Throttling State  Description  Query
Pkt Dropped  Resp Pkt Dropped
-----
0.02(3)                MDNS_NO_THROTTLING  No packets dropped  0
      0

```

The following example displays the detailed statistics of packets sent and received per second by AirGroup:

```

(host) [mynode] ##show airgroup internal-state statistics verbose

Time: Tue Jul 12 13:27:59 2016
PAPI Messages
-----
Msg ID  Name                                Sent Since last Read  Sent Total  Recv Since
Last Read  Recv Total

```

Id	Message	Sent	Since Last Read	Recv
7062	Set switch ip6 1	0		0
7064	Set vlan ipv6 info 1	0		0
65534	sapi getstate response 1	0		0
7005	Set switch ip 1	0		0
14001	mdns cli request 331	0		1

RADIUS Client Messages

Type	Sent	Since Last Read	Sent Total	Recv Since Last
Read Recv Total				
Auth Req/Resp 13823	0		30223	0
RFC3576 0	N/A		N/A	0
CPPM Device-Entry Added 2	N/A		N/A	0
CPPM Device-Entry Deleted 0	N/A		N/A	0

MDNS Messages

Opcode	Name	Sent	Since Last Read	Sent Total	Recv
Since Last Read	Recv Total				
7	app 0	0		5	0
-	SDN 4152	0		11092	0
Rx	Request 591	N/A		N/A	0
Rx	Response 556	N/A		N/A	0
Tx	Request-Refresh N/A	0		10106	N/A
Tx	Request-discovery N/A	0		1836	N/A
Tx	Request-wildcard N/A	0		0	N/A
Tx	Response-Solicited N/A	0		0	N/A
Tx	Response-Solicited-Fragment N/A	0		0	N/A
Tx	Response-Unsolicited N/A	0		0	N/A
Tx/Rx	Total N/A	0		0	N/A

DLNA Messages

Opcode	Name	Sent	Since Last Read	Sent Total	Recv	Since Last
Read	Recv Total					
-	SDN 967567	0		366195	8	
Rx	Query 838110	N/A		N/A	8	
Rx	Notify Announce 69490	N/A		N/A	0	
Rx	Notify Bye 6	N/A		N/A	0	
Tx	Response N/A	0		33958	N/A	

Internal MDNS Statistics

Functionality	Hit Count	Since Last Read	Hit Count Total
Response - Cache Update	0		3176
Response	0		556
Query - prepare records + Policy	0		591
Query - Policy	0		12
Query - resp pkt gen & send	0		0
Query - Response packet send	0		331387
Query	0		591
Multicast Response propagate	0		0

Internal DLNA Statistics

Functionality	Hit Count	Since Last Read	Hit Count Total
Response - Cache Update	0		73961
Response	0		0
Query - prepare records + Policy	0		14227
Query - Policy	0		34360
Query - resp pkt gen & send	0		14170
Query - Response packet send	0		74437
Query	8		838110

MDNS Multi-controller Cluster Messages

Type	Sent	Since Last Read	Sent Total	Recv
Since Last Read	Recv Total			
Unicast Response with tag 0	0		0	0
Request with tag 0	0		0	0
Raw Response 0	0		0	0

Multicast Propagate Raw Response 0 0 0
0

DLNA Multi-controller Cluster Messages

Type	Sent Since Last Read	Sent Total	Recv Since Last Read	
Request with tag	0	0	0	0
Raw Response	0	0	0	0

Packet Arrival Statistics (per minute)

Peak Packet Arrival Rate	Peak Arrival Time	No. Servers	No. Clients
454	Jul 05 10:34:42	5	16

Cache Bucket Size

Service	AP Name Bucket	AP FQLN Bucket	User Name Bucket	Default Bucket
MDNS	0	0	0	1
SSDP	0	0	0	4

Internal mDNS and DLNA Thread Statistics

#	Thread ID	Query since Last Read	Queries Recv Total	Queries in Queue
1	3368556288	2	489191	0
6				
2	3343378176	4	92394	0
10				
3	3318200064	0	74189	0
2				
4	3293021952	0	110019	0
11				
5	3267843840	2	72908	0
2				

MDNS CPU and Throttling details

Current CPU Utilization (%)	Throttling State	Description	Query
0.03(3)	MDNS_NO_THROTTLING	No packets dropped	0

list of controllers in same vlan

Controller MAC
00:1a:1e:01:ae:28

```
00:0b:86:b5:15:97
00:1a:1e:01:99:e0
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bf:70
00:1a:1e:02:07:b0
00:0b:86:9a:4e:77
00:0c:29:10:8c:b8
00:0b:86:b8:e1:d8
00:1a:1e:01:bd:b0
```

```
list of local controllers with AirGroup devices
```

```
-----  
Controller MAC
```

```
-----  
00:0b:86:9a:4a:37  
00:0c:29:d7:6d:e3  
00:1a:1e:01:bd:b0
```

```
AirGroup users 10, AirGroup servers 5. Total devices 36
```

Related Commands

Command	Description
airgroup	This command configures AirGroup settings.
airgroupprofile	This command configures an AirGroup profile.
show aigroup	This command shows the global AirGroup settings.
show aigroupprofile	This command shows the AirGroup profile settings.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show airmatch tech-support

```
show airmatch tech-support
  ap-name <name>
  mac <mac>
```

Description

This command collects the output for the AP or the radio for further support or engineering analysis. You can add a file name at the end of this command to capture the output to the flash.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch technical support data.
mac <mac>	MAC ID of an AP for which you want to view AirMatch technical support data.

Example

The following example displays the output of the `show airmatch tech-support mac ac:a3:1e:59:b4:c0` command:

```
(host) [mynode] #show airmatch tech-support mac ac:a3:1e:59:b4:c0

show airmatch debug reporting-radio MAC ac:a3:1e:59:b4:c0
Field                               Value
-----                               -
Band                                 2GHz
AP Ethernet MAC                      ac:a3:1e:cd:9b:4c
Radio MAC                            ac:a3:1e:59:b4:c0
AP Name                              F-16-a-QCA
AP Model                             AP-325
LMS IP                               192.168.200.15
Switch IP                            192.168.200.15
Last Update                          2017-11-16 02:57:57
Channel                              7
Bandwidth                            20MHz
Channel Reason                       AirMatch - Solver
Channel Update Time                  2017-11-14 10:42:53
EIRP                                 10.0 (dBm)
EIRP Reason                          AirMatch - Solver
EIRP Update Time                    2017-11-16 02:55:19
Is Active                            true
Is Static Chan                       false
Is Static EIRP                       false
Is Static CSR                        false
Deploy Hour                          N/A
```

```

Retries          5
Last Retry Time  2017-11-14 09:00:38
Local Time       PST8PDT,M3.2.0,M11.1.0
show airmatch debug optimization MAC ac:a3:1e:59:b4:c0
# 2017-11-15_08:00:36      Scheduled
# 5GHz   network cost/solution cost: 6.8/5.4
# 2.4GHz network cost/solution cost: 16.2/14.1
# Band Radio          RFDom Part  Chan  CBW      EIRP (dBm)  APName
ID      ID
-----
2GHz ac:a3:1e:59:b4:c0 001    000     3i    20i     10.0    F-16-a-QCA
[*] regarded frozen | [i] channel ignored because insufficient quality
increase | [t] EIRP truncated

show airmatch debug solution MAC ac:a3:1e:59:b4:c0
# Band Radio          Chan/Opt#  CBW      EIRP (dBm)/Opt#  Chan Time
      EIRP Time          Confirm Time      Retries  APName
-----
2GHz ac:a3:1e:59:b4:c0      7 / 193      20      10.0 / 193 2017-11-14_
10:42:46 2017-11-14_10:42:46 2017-11-14_10:57:46      0 F-16-a-QCA
[*] regarded frozen | [#] result adjusted to match feasibility
show airmatch debug feasibility MAC ac:a3:1e:59:b4:c0
AirMatch Radio Feasibility Band 2GHz for current opmode DUAL_BAND
-----
Field                Value
-----
Mac                   ac:a3:1e:59:b4:c0
Updated On            2017-11-16 02:37:28
Current Opmode        DUAL_BAND
HW Supported Opmodes  DUAL_BAND
Configured Opmodes    DUAL_BAND,DUAL_5G
Feasible Opmodes      DUAL_BAND
Chan 20MHz            3,7,9
Chan 40MHz
Chan 80MHz
Chan 160MHz
Bandwidth             20MHz
Config BW range(MHz) 20 - 20
Hardware BW range(MHz) 20 - 40
Eirp Range Chan 20MHz 3:[9,12] 7:[9,12] 9:[9,12]
Eirp Range Chan 40MHz
Eirp Range Chan 80MHz
Eirp Range Chan 160MHz
EIRP (dBm)            9 - 12
Config EIRP range (dBm) 6 - 12
Hardware EIRP range (dBm) 9 - 26
EIRP Offset (dB)     0
Band                  2GHz
Band Range            BAND_FULL
Update Reason         Periodic Update
Last Update           2017-11-16 02:37:28

show airmatch debug solver feasibility optimization 194 MAC
ac:a3:1e:59:b4:c0
Field                Value

```


ac:a3:1e:59:98:20	*	77	9	2017-11-16
02:55:19	F-Multiclient-a			
ac:a3:1e:59:9e:00	*	77	3	2017-11-16
02:55:19	F-12			
18:64:72:d3:81:00	*	78	7	2017-11-16
02:55:19	F-11-BRCM			
ac:a3:1e:59:aa:a0	*	78	3	2017-11-16
02:55:19	F-13			
9c:1c:12:87:33:60	*	79	9	2017-11-16
02:55:19	F-4-BRCM			
a8:bd:27:d0:5f:c0	*	79	3	2017-11-16
02:55:19	F-19-b			
a8:bd:27:d0:5e:80	*	81	3	2017-11-16
02:55:19	F-19-a			
9c:1c:12:8c:6e:a0	*	84	7	2017-11-16
02:55:19	Fremont-sniffer-225			
a8:bd:27:59:fc:e0	*	84	9	2017-11-16
02:55:19	F-19-c			
ac:a3:1e:59:9e:80	*	88	9	2017-11-16
02:55:19	F-front-door-1			
c8:b5:ad:bb:13:c0	*	90	11	2017-11-13
15:44:15	F3-345			
a8:bd:27:59:fb:e0	*	91	3	2017-11-14
22:03:56	a8:bd:27:cd:9f:be			
c8:b5:ad:bb:15:00	*	96	11	2017-11-13
15:44:15	F8-345			
b4:5d:50:6c:a6:c0		42	1	2017-11-16
02:55:19				
70:3a:0e:32:b7:08		53	1	2017-11-14
16:18:53				
70:3a:0e:32:b7:00		62	1	2017-11-16
02:55:19				
70:3a:0e:52:10:80		63	1	2017-11-16
02:55:19				
84:d4:7e:61:f9:a0		67	6	2017-11-16
02:55:19				
ac:a3:1e:b4:a3:00		67	1	2017-11-16
02:55:19				
40:e3:d6:bf:12:a0		67	1	2017-11-15
16:57:15				
c8:b5:ad:1f:c5:c8		67	11	2017-11-14
08:55:52				
34:fc:b9:fd:4b:a8		68	11	2017-11-14
08:55:52				
34:fc:b9:fd:4b:a0		69	11	2017-11-16
02:55:19				
b4:5d:50:6c:a6:c8		69	11	2017-11-14
08:55:52				
b4:5d:50:83:43:60		70	1	2017-11-16
02:55:19				
c8:b5:ad:1f:c5:c0		70	6	2017-11-16
02:55:19				
b4:5d:50:83:43:68		71	1	2017-11-16
02:55:19				
b4:5d:50:6c:a8:00		71	1	2017-11-16
00:49:09				

9c:1c:12:8c:6d:08 16:15:59	72	11	2017-11-13
9c:1c:12:8c:6d:00 02:55:19	74	11	2017-11-16
c8:b5:ad:bb:01:28 08:55:52	74	6	2017-11-14
34:fc:b9:d3:53:80 02:55:19	75	1	2017-11-16
b4:5d:50:db:f0:c0 02:55:19	75	11	2017-11-16
18:64:72:25:76:a0 00:49:10	76	11	2017-11-16
70:3a:0e:32:b9:a0 06:26:42	78	1	2017-11-15
24:de:c6:2f:64:c0 02:55:19	79	6	2017-11-16
08:ea:44:83:a4:50 15:44:15	79	1	2017-11-13
08:ea:44:99:ad:10 02:55:19	80	6	2017-11-16
24:de:c6:2f:65:40 02:55:19	81	6	2017-11-16
34:fc:b9:fd:4c:40 11:35:13	87	1	2017-11-14
84:d4:7e:61:f9:a8 08:55:52	87	6	2017-11-14
ac:a3:1e:55:80:a0 02:55:19	89	1	2017-11-16
00:21:43:46:2b:30 16:50:00	92	6	2017-11-14
f0:5c:19:1c:6a:a0 10:31:24	93	11	2017-11-14
f0:5c:19:1c:6a:a8 10:31:24	93	11	2017-11-14
c8:b5:ad:bb:01:20 08:55:52	93	6	2017-11-14
a8:bd:27:d0:65:20 08:55:52	94	11	2017-11-14
a8:bd:27:d0:65:28 08:55:52	94	11	2017-11-14
a8:bd:27:59:f0:20 10:31:24	96	6	2017-11-14
a8:bd:27:59:f0:28 10:31:24	96	6	2017-11-14
6c:f3:7f:e7:67:e0 09:59:29	97	6	2017-11-14
40:e3:d6:7f:48:08 09:27:25	97	6	2017-11-14
0a:8d:db:84:92:10 08:01:17	97	11	2017-11-14
0c:8d:db:84:92:10 08:01:17	97	11	2017-11-14
40:e3:d6:7f:48:00 08:55:52	98	11	2017-11-14
6c:f3:7f:e7:67:e8 08:55:52	98	11	2017-11-14

```

94:b4:0f:f3:1d:00      98      11      2017-11-14
08:55:52
94:b4:0f:f3:1d:08      98      11      2017-11-14
08:55:52
ac:a3:1e:b4:a3:08      98      6       2017-11-14
08:55:52
b4:5d:50:6c:a2:c0      99      1       2017-11-15
00:09:35
d8:50:e6:58:9b:48     101     10      2017-11-16
02:55:19
e2:55:7d:78:75:48     102     6       2017-11-14
17:52:51
f8:32:e4:54:8a:f8     104     6       2017-11-16
02:55:19
ac:9e:17:a9:be:30     107     10      2017-11-14
05:55:07
24:a4:3c:04:03:28     107     1       2017-11-13
07:46:59
2e:a4:3c:04:03:28     107     1       2017-11-13
07:46:59
32:a4:3c:04:03:28     108     1       2017-11-13
15:44:15
2e:a4:3c:04:01:70     109     11      2017-11-14
09:59:29
00:1e:e5:2c:87:38     109     11      2017-11-13
15:44:15
70:77:81:45:42:68     109     6       2017-11-13
07:46:59
2a:a4:3c:04:00:a8     110     6       2017-11-13
09:23:08
2e:a4:3c:04:00:a8     110     6       2017-11-13
07:46:59
32:a4:3c:04:00:a8     110     6       2017-11-13
07:46:59
2a:a4:3c:04:01:70     111     11      2017-11-14
08:55:52
32:a4:3c:04:01:70     111     11      2017-11-14
08:55:52
24:a4:3c:04:01:70     111     11      2017-11-14
08:01:17
c8:6c:87:fe:94:40     111     1       2017-11-13
14:09:39
24:a4:3c:04:00:a8     111     6       2017-11-13
07:46:59
00:90:4a:c1:01:f0     112     11      2017-11-14
08:55:52

```

```

show airmatch debug history MAC ac:a3:1e:59:b4:c0
2GHz radio mac ac:a3:1e:59:b4:c0 ap name F-16-a-QCA

```

```

-----
Time of Change      Chan      Bandwidth      EIRP (dBm)      Mode
Source
-----
- -----

```

```

2017-11-14 15:42:46      3->      7      20->    20      9.0-> 10.0    AP ->AP
  Solver
2017-11-14 15:25:34      6->      1      20->    20     10.0->  9.0    AP ->AP
  Solver
2017-11-14 13:26:47     11->      6      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-11-13 13:08:15      6->     11      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-11-12 21:00:52      6->      6      20->    20     11.0-> 10.0    AP ->AP
  Solver
2017-11-11 21:00:42      6->      6      20->    20     10.0-> 11.0    AP ->AP
  Solver
2017-11-08 21:00:41      6->      6      20->    20     11.0-> 10.0    AP ->AP
  Solver
2017-11-06 21:00:41      6->      6      20->    20     10.0-> 11.0    AP ->AP
  Solver
2017-11-05 21:00:42      6->      6      20->    20     11.0-> 10.0    AP ->AP
  Solver
2017-11-03 21:00:31      6->      6      20->    20     10.0-> 11.0    AP ->AP
  Solver
2017-11-02 20:26:18      1->      6      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-28 02:14:06      6->      1      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-28 02:09:35      1->      6      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-27 13:00:27      1->      1      20->    20      9.0-> 10.0    AP ->AP
  Solver
2017-10-26 21:53:06      6->      1      20->    20     10.0->  9.0    AP ->AP
  Solver
2017-10-25 20:31:48      1->      6      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-25 18:40:22      6->      1      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-25 18:29:11     11->      6      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-25 17:59:59      1->     11      20->    20     10.0-> 10.0    AP ->AP
  Solver
2017-10-25 17:06:55     11->      1      20->    20      9.0-> 10.0    AP ->AP
  Solver
show airmatch event radar MAC ac:a3:1e:59:b4:c0
No events found for bssid ac:a3:1e:59:b4:c0
show airmatch event noise MAC ac:a3:1e:59:b4:c0
No events found for bssid ac:a3:1e:59:b4:c0

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.

Command	Description
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch network-tech-support

```
show airmatch network-tech-support
  ap-name <name>
  band <bandname> {2.4GHz|5GHz} <rf-domain>
  mac <mac>
```

Description

This command collects the output for all the radios that are in the same partition for a specified radio AP name. This command also lists and describes the AP radios that are handled further. Run this command to collect the output for further support or engineering analysis. You can add a file name at the end of this command to capture the output to the flash.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch network support data
band	Radio type based on which the AP operates 2.4GHz to 5GHz
mac <mac>	MAC address an AP for which you want to view AirMatch network support data

Example

The following example displays a partial output of the `show airmatch network-tech-support ap-name F-16-a-QCA` command:

```
(host) [mynode]#show airmatch network-tech-support ap-name F-16-a-QCA
```

```
# Summary of included radios
# AP Name: F-16-a-QCA  Radio: ac:a3:1e:59:b4:c0  Band: 2GHz  RF domain: 001
partition: 000
# Num radios: 40  New radios: false
# Radio          AP Name
-----
ac:a3:1e:59:b4:c0  F-16-a-QCA
a8:bd:27:d0:69:e0  F-PP-a-QCA
9c:1c:12:8c:6e:a0  Fremont-sniffer-225
ac:a3:1e:59:9e:00  F-12
70:3a:0e:52:22:40  F-PP-b
ac:a3:1e:59:c7:80  F-16-c-QCA
ac:a3:1e:59:97:e0  F-RVR-d
ac:a3:1e:59:98:20  F-Multiclient-a
70:3a:0e:52:23:a0  F-17-QCA
a8:bd:27:d0:5e:80  F-19-a
70:3a:0e:52:28:e0  F-15-a
```

```

18:64:72:7e:af:20 F-15-b-QCA
a8:bd:27:59:fc:e0 F-19-c
a8:bd:27:59:fc:00 F-18-c
a8:bd:27:59:f4:e0 F-18-b
ac:a3:1e:59:aa:a0 F-13
a8:bd:27:d0:5f:c0 F-19-b
ac:a3:1e:53:b8:00 F-16-b-QCA
ac:a3:1e:59:b7:40 F-RVR-g
a8:bd:27:59:fb:e0 a8:bd:27:cd:9f:be
18:64:72:fd:67:a0 18:64:72:c7:d6:7a
18:64:72:d3:81:00 F-11-BRCM
ac:a3:1e:59:9e:80 F-front-door-1
9c:1c:12:87:33:60 F-4-BRCM
ac:a3:1e:59:9d:00 F-RVR-e
ac:a3:1e:59:9a:c0 F-14-QCA
70:3a:0e:6e:5e:20 F-RVR-b
a8:bd:27:d0:94:a0 F-18-a
ac:a3:1e:59:a0:00 1344-2-AP04
18:64:72:7e:c5:c0 F-15-c-QCA
# AP Name: F-16-a-QCA Radio: ac:a3:1e:59:b4:d0 Band: 5GHz RF domain: 001
partition: 000
# Num radios: 49 New radios: false
# Radio AP Name
-----

```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch optimization

show airmatch optimization <seq>

Description

This command displays the list of recent RF optimization jobs performed by AirMatch.

Parameter	Description
<seq>	Specify a sequence number to view details for a specific AirMatch solution.

Example

The following example shows the history AirMatch solutions for 5 GHz and 2 GHz radios.

```
(host) *[mynode] #show airmatch optimization
Seq Time           APs [5GHz] Radios Cost Conflict Deploy [2GHz]
Radios Cost Conflict Deploy Type
-----
#14 20161025_05:04:53 3          3 2.2 0.0 No
    0 0.0 0.0 No Scheduled
#13 20161024_05:04:53 3          3 2.2 0.0 No
    0 0.0 0.0 No Scheduled
#12 20161023_05:04:50 3          3 2.2 0.0 No
    0 0.0 0.0 No Scheduled
#11 20161022_05:04:50 3          3 2.2 0.0 Yes
    0 0.0 0.0 No Scheduled
#10 20161020_10:12:59 2          2 2.0 0.0 Yes
    0 0.0 0.0 Yes On-demand
#9  20161020_09:20:23 2          2 2.0 0.0 Yes
    0 0.0 0.0 Yes Quick
#8  20161020_09:19:27 2          2 2.0 0.0 Yes
    0 0.0 0.0 Yes On-demand
```

The output of the `show airmatch optimization` command includes the following parameters:

Column	Description
Seq	Sequence number of the solution. The solution with the highest sequence number is the most recent.
Time	Timestamp showing the date and time AirMatch sent the solution update

Column	Description
APs	Number of APs updated with the new solution
Radios	Number of 5 Ghz or 2 Ghz AP radios updated with the new solution.
Capacity	Capacity is an internal metric to track the quality of a solution. The higher the capacity, the better the solution.
Cost	Cost is an internal metric to track the cost of a solution or a network state. The lower the cost, the better the solution. It is a measure of the overall quality of the solution or the network state.
Conflict	Conflict is an internal metric to track the quality of a solution. The lower the conflict, the better the solution.
Deploy	This column displays a status of Yes if the improvement in the radio band met or exceeded the threshold for deployment. If this column displays a status of No , the solution was below the quality threshold and was not deployed.

To see the detail of channel and EIRP plan for all the radios in the network, append the solution sequence number in the same command.

```
(host) [mm/mynode] #show airmatch optimization 14
# 20161025_05:04:53      Scheduled
# 5GHz   capacity/network cost/solution cost/improvement: 11.0/2.2/2.2/0.0%
# 2.4GHz capacity/network cost/solution cost/improvement: 0.0/0.0/0.0/0.0%
# Band Radio              Mode Chan  CBW    EIRP (dBm)  APName
-----
5GHz 84:d4:7e:d2:10:90 AP    36*   160*     5*  ap315-1
5GHz 9c:1c:12:88:6c:70 AP    157i   40i    12.  ard4
5GHz 18:64:72:7e:4d:90 AP    149*   20*     5*  x4p3
[*] regarded frozen | [.] no change | [i] channel ignored because
insufficient quality increase
```

A radio is regarded frozen if any of the following are true:

- The CLI command `airmatch ap freeze` command has been used to configure and freeze radio settings
- The radio's regulatory domain profile leads to a single feasible channel by allowing only single valid channel, channel pair, or channel group.
- Neighboring radar and/or channel noise makes only a single channel feasible.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch profile

```
show airmatch profile
```

Description

This command displays the configuration settings in the AirMatch profile.

Example

In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, the output appears in a single, long table.

```
(host)[mm] #show airmatch profile
AirMatch profile (Predefined (changed))
-----
Parameter          Value
-----
schedule           Enabled
deploy-hour        5 o'clock
quality-threshold  15 percent
```

The output of this command includes the following parameters:

Column	Description
Schedule	Indicates if AirMatch scheduled updates are enabled. If the AirMatch updates are changed from the default enabled setting to disabled , the Mobility Conductor continues to receive RF updates from the APs, but no channel and EIRP changes are executed by the Mobility Conductor at the scheduled time.
deploy-hour <0-23>	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format).
eirp-offset	Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm
quality-threshold	The <code>quality-threshold</code> parameter represents the percentage of channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change does not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>eirp-offset</code> parameter is deprecated. EIRP offset values can now be configured for AP groups via the rf dot11a-radio-profile and rf dot11g-radio-profile commands.
ArubaOS 8.0.1.0	The <code>quality-threshold</code> parameter is introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airmatch solution

```
show airmatch solution
  ap-name <ap-name>
  band <band>
  list-all
  mac <mac-addr>
  switch-ip
```

Description

This command displays history of AirMatch solution updates.

Parameter	Description
ap-name <ap-name>	Specify the name of an AP with the <ap-name> parameter to view AirMatch solutions for the radios on that AP.
band <band>	Specify the radio band for an AP as either 2 GHz, 5 GHz, or 6 GHz to view AirMatch solutions for that radio .
list-all	Show AirMatch solutions for all devices.
mac <mac-addr>	Show AirMatch solutions for a specific AP radio by entering the MAC address of the radio.
switch-ip <switch-ip>	Specify the IP address of the switch to view AirMatch solutions for that switch.

Example

The following example shows the history of AirMatch solutions.

```
(RagSC) ^[mynode] #show airmatch solution list-all

# Band Radio              Chan/Opt#    CBW      EIRP (dBm) /Opt# Client Band
APName                                     Pref  Pref
-----
-----
6GHz 34:8a:12:2e:df:40      37 / 88     80       15.0 / 114     a     F
APX_01_615
6GHz 34:8a:12:2e:e5:00     181 / 88    80       15.0 / 114     a     F
APU_01_615
6GHz 34:8a:12:2e:e7:80     165 / 88    80       15.0 / 114     a     F
APJ_01_615
6GHz 34:8a:12:2f:05:20     53 / 88     80       15.0 / 114     a     F
APN_01_615
```

6GHz 34:8a:12:2f:1d:c0	213 / 88	80	15.0 / 114	a	F
APO_01_615					
6GHz 34:8a:12:f7:be:50	85 / 138	80	15.0 / 142	a	F
APQ_01_6					
6GHz 34:8a:12:f7:d5:90	133 / 138	80	15.0 / 142	a	F
APR_01_655					
6GHz 34:8a:12:f7:f4:b0	165 / 138	80	15.0 / 142	a	F
APF_01_655					
6GHz 94:64:24:8a:d5:d0	69 / 138	80	15.0 / 142	a	F
APK_12_635					
6GHz cc:88:c7:40:53:c0	101 / 88	80	15.0 / 114	a	F
APA_01_615					
6GHz cc:88:c7:40:54:20	117 / 88	80	15.0 / 114	a	F
APD_01_615					
6GHz cc:88:c7:41:54:10	53 / 138	80	15.0 / 142	a	F
APB_01_635					
6GHz cc:88:c7:41:85:30	213 / 138	80	15.0 / 142	a	F
APF_11_635					

The output of the **show airmatch solution** command includes the following parameters:

Column	Description
Band	Frequency band used by the radio
Radio	MAC address of an AP radio
Chan/Opt#	Channel from optimization Opt #, and the new optimization sequence ID applied by the solution. If no change was made, the Opt# column displays the value "NA".
CBW	Channel bandwidth used by the radio.
EIRP/Opt#	EIRP from optimization Opt #, and the optimization sequence ID applied by the solution. If no change was made, the Opt# column displays the value "NA".
Client Pref	Client preference from one of the following: <ul style="list-style-type: none"> ■ [p] HE Preferred ■ [n] Non-HE Preferred ■ [a] Allow-All
Band Pref	Band preference from one of the following: <ul style="list-style-type: none"> ■ [L] 5GHz-Lower ■ [U] 5GHz-Upper ■ [F] 5GHz-Full
AP_name	Name of the AP.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output for AP-555 access points will display details of Radio 2.
ArubaOS 8.1.0.0	The output of this command has been modified to include channel and EIRP information. The information that appeared in the output of this command in previous versions of ArubaOS now appear in the command show airmatch optimization .
ArubaOS 8.0.1.0	The output of this command is updated to include the following parameters for each radio band: <ul style="list-style-type: none"> ■ capacity ■ network cost ■ solution cost ■ improvement data
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show airslice

```
show airslice-profile <name>
show airslice-visibility
  client [table | <mac> ]
  debug counters
  record-limit
```

Description

This command displays the details of Air Slice profile.

Parameter	Description
airslice-profile <name>	Displays the Air Slice profile configuration details.
airslice-visibility	Displays the details of applications.
client table	Displays the details of applications used by clients.
client <mac>	Displays the details of applications used by a specific client.
debug counters	Copies data from another Air Slice profile.
no	Displays the debug counters of AirSlice visibility.
record-limit	Displays the configured record limit for clients.

Example

The following command displays the configured record limit of an Air Slice profile:

```
(host) [mynode] #show airslice-visibility record-limit
                 airslice-visibility record-limit :100
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Air Slice is supported on all 802.11ax APs. However, Air Slice is supported only on 5 GHz radio and not on 6 GHz radio for 630 Series access points.	Base operating system.	Config and Enable mode on Mobility Conductor.

show ale-configuration

```
show ale-configuration
```

Description

This command displays ALE configuration on the Mobility Conductor.

Example

```
To display the ALE configuration:  
(host) [mynode] (config) #show ale-configuration  
  
Anonymization: false  
ALE Server-1: none  
ALE Server-2: none  
ALE Server-3: none  
ALE Server-4: none  
ALE Server-5: none  
nbapi_publish: true  
ale_sta_assoc: false
```

Related Command

Command	Description
ale-configuration	Enable ALE configuration and its parameters on the Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show allowed-address-list

```
show allowed-address-list
  all
  ipv4
  ipv6
```

Description

This command displays the list of allowed IPv4 or IPv6 addresses that are exempted.

Parameter	Description
all	This parameter displays all the IP addresses in the allowed address list.
ipv4	This parameter displays the IPv4 addresses in the allowed address list.
ipv6	This parameter displays the IPv6 addresses in the allowed address list.

Related Commands

Command	Description
allowed-address-list	This command configures addresses exempted when the deny-inter-user-bridging is enabled.
no allowed-address-list	This command is used to remove the IP addresses that were added using allowed-address-list command.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and Managed Device.

show amon msg-buffer-size

```
show amon msg-buffer-size
```

Description

This command displays the size of AMON packets on the managed device.

Example

The following command displays size of AMON packet:

```
(host) [mynode] #show amon msg-buffer-size
amon msg-buffer-size :1264
```

Related Commands

Command	Description
amon msg-buffer-size	Modifies the size of AMON packets on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show amon-receiver

```
show amon-receiver [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-  
stats-inst-1] | [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] |  
[dest-stats-inst-5] | [dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] |  
[error-counters] | [error-counters-all] | [interest-table] | [list-details] |  
[parameter] | [set-debug-level-dest] | [src-stats-all] | [stats-counters] | [stats-  
counters-all]]
```

Description

This command displays AMON receiver information.

Parameter	Description
dest-stats	Shows destination statistics
dest-stats-all	Shows all destination statistics
dest-stats-inst-0	Shows destination statistics instance 0
dest-stats-inst-1	Shows destination statistics instance 1
dest-stats-inst-2	Shows destination statistics instance 2
dest-stats-inst-3	Shows destination statistics instance 3
dest-stats-inst-4	Shows destination statistics instance 4
dest-stats-inst-5	Shows destination statistics instance 5
dest-stats-inst-6	Shows destination statistics instance 6
dest-stats-inst-7	Shows destination statistics instance 7
dest-table	Shows destination table
error-counters	Shows error counters
error-counters-all	Show all error counters
interest-table	Show interest table
list-details	Show list details
parameter	Shows parameter String
set-debug-level-dest	Shows the set debug level for destination
src-stats-all	Shows all source statistics

Parameter	Description
stats-counters	Shows stats counters
stats-counters-all	Shows all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] #show amon-receiver dest-stats-inst-0

AMON-RECEIVER
dest_id 0: port 15260
-----
  Id: MsgName                Mode      NoOfMsgs   NoOfBytes
-----
  0: RADIO_STATS              UDS        44807      48570788
  1: VAP_STATS                 UDS        32958      31730709
  2: STATION_STATS            UDS       1733704    2136005092
 10: USER_INFO                 UDS        26735      22146508
 11: AP_INFO                   UDS         18         13662
 12: RADIO_INFO                UDS         22         2952
 13: VAP_INFO                   UDS         17         3138
 47: CLUSTER_SELF_NODE_INFO    UDS        26919      3822498
 48: CLUSTER_SELF_NODE_STATS    UDS        26913      4225341
 49: CLUSTER_PEER_NODE_INFO     UDS        80757     13163391
 50: CLUSTER_PEER_NODE_STATS    UDS        26913      7158858
 67: HWMON_TEMP_DETAIL          UDS        30881     15625786
 68: HWMON_FAN_DETAIL           UDS        30881     6176200
 69: HWMON_SENSOR_THRS          UDS        30881     4539507
 70: HWMON_SENSOR_VAL           UDS        30881     5280651
 71: HWMON_SYS_INFO             UDS        48802     47923564
 72: FPAPPS_PORTS_INFO          UDS       107618     12914160
 73: FPAPPS_PORT_DETAIL          UDS       538030     497677750
 74: FPAPPS_PC_DETAIL_MESSAGE    UDS       860947     846310901
 75: FPAPPS_CTRL_INFO           UDS       107617     10008381
 76: FPAPPS_CTRL_IP             UDS       107619     8824758
-----
Total [ 21 messages]                3893920   3722124595
-----

reclaim_reason_conn_not_ready : 0
no_of_times_punished           : 0

Start time      : Thu Jul  7 09:29:17 2016
Last Cleared time : Thu Jul  7 09:29:17 2016
Current time    : Wed Jul 13 15:06:07 2016 (Elapsed time: 538610)
```

Related Commands

Command	Description
clear amon-receiver	This command displays AMON receiver information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show amon-sender

```
show amon-sender
  bundle counters
  bundle parameters
  cdt message-type <msgtype>
  dest-stats-all
  dest-stats-all-all
  dest-stats-inst-0
  dest-stats-inst-1
  dest-stats-inst-2
  dest-stats-inst-3
  dest-stats-inst-4
  dest-stats-inst-5
  dest-stats-inst-6
  dest-stats-inst-7
  dest-table
  egress-counters
  error-counters
  error-counters-all
  filter
  filters
  ingress-counters
  interest-table
  list-details
  parameter
  set-debug-level-dest
  src-stats-all
  src-stats-all-all
  stats-counters
  stats-counters-all]
```

Description

This command displays AMON sender information. This command must be run on the managed device.

Parameter	Description
bundle counters	Shows the number of messages, records, and bytes in a bundle
bundle parameters	Shows the parameters that are in a bundle
cdt message-type <msgtype>	shows the column descriptor table for the specified AMON message number
dest-stats-all	Shows all destination statistics

Parameter	Description
dest-stats-all-all	Shows all destination statistics including entries with zero messages
dest-stats-inst-0	Shows destination statistics instance 0
dest-stats-inst-1	Shows destination statistics instance 1
dest-stats-inst-2	Shows destination statistics instance 2
dest-stats-inst-3	Shows destination statistics instance 3
dest-stats-inst-4	Shows destination statistics instance 4
dest-stats-inst-5	Shows destination statistics instance 5
dest-stats-inst-6	Shows destination statistics instance 6
dest-stats-inst-7	Shows destination statistics instance 7
dest-table	Shows destination table
egress-counters	Shows egress counters
error-counters	Shows error counters
error-counters-all	Show all error counters
filter	Filter Information
filters	Show smart-amon filters
ingress-counters	Show ingress counters
interest-table	Show interest table
list-details	Show list details
parameter	Shows parameter String
set-debug-level-dest	Shows the set debug level for destination
src-stats-all	Shows all source statistics
src-stats-all-all	Shows all source statistics including entries with zero messages
stats-counters	Shows stats counters
stats-counters-all	Shows all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] # logon 192.0.1.12
(host) [MDC] # show amon-sender dest-stats-inst-0

AMON SENDER STATS
-----
AMON-SENDER
dest_id 0: 192.0.1.12
-----

```

Id	MsgName	Mode	NoOfMsgs	NoOfBytes
0:	RADIO_STATS	UDP	17979	19489236
1:	VAP_STATS	UDP	9578	11258881
2:	STATION_STATS	UDP	325693	401740468
7:	FW_AGG_SESSIONS	UDP	190028	217222300
9:	FW_APP	UDP	507	625776
10:	USER_INFO	UDP	2443	2087840
11:	AP_INFO	UDP	16	12144
12:	RADIO_INFO	UDP	15	2064
13:	VAP_INFO	UDP	13	2460
18:	AP_SYSTEM_STATS	UDP	9578	756824
26:	FW_APP_CATEGORY	UDP	2	1784
27:	FW_WEB_CC_CATEGORY	UDP	5	5500
29:	DHCP_STATION_INFO	UDP	39048	37218948
32:	DOT1X	UDP	1579	687868
33:	WPA_KEY_HANDSHAKE	UDP	1527	282978
36:	PASSIVE_CTRL_STA_STATS	UDP	173	36916
45:	GEN_DATA	UDP	4483	5254076
47:	CLUSTER_SELF_NODE_INFO	UDP	9005	1278710
48:	CLUSTER_SELF_NODE_STATS	UDP	9002	1413314
49:	CLUSTER_PEER_NODE_INFO	UDP	27022	4404586
50:	CLUSTER_PEER_NODE_STATS	UDP	9002	2394904
67:	HWMON_TEMP_DETAIL	UDP	8149	4123394
68:	HWMON_FAN_DETAIL	UDP	8149	1629800
69:	HWMON_SENSOR_THRS	UDP	8149	1197903
70:	HWMON_SENSOR_VAL	UDP	8149	1393479
71:	HWMON_SYS_INFO	UDP	8149	8002318
72:	FPAPPS_PORTS_INFO	UDP	18000	2160000
73:	FPAPPS_PORT_DETAIL	UDP	108000	99900000
74:	FPAPPS_PC_DETAIL_MESSAGE	UDP	144000	141552000
75:	FPAPPS_CTRL_INFO	UDP	18000	1674000
76:	FPAPPS_CTRL_IP	UDP	18000	1476000
Total [31 messages]			1003443	969286471

```
-----
reclaim_reason_conn_not_ready : 0
no_of_times_punished          : 0

Start time      : Sat Jul  9 23:23:47 2016
Last Cleared time : Sat Jul  9 23:23:47 2016
Current time    : Sat Jul 16 05:32:16 2016 (Elapsed time: 540509)

(host) [mynode] # logon 0: 2001:0000:0000:0000:0000:0000:0000:0002
(host) [MDC] # show amon-sender dest-stats-inst-0
```

AMON-SENDER

dest_id 0: 2001:0000:0000:0000:0000:0000:0000:0002

Id: MsgName	Mode	NoOfMsgs	NoOfBytes
0: RADIO_STATS	DTLS	333707	377756324
1: VAP_STATS	DTLS	167371	143436947
2: STATION_STATS	DTLS	1296493	1120169952
7: FW_AGG_SESSIONS	DTLS	3382882	3903824624
9: FW_APP	DTLS	522	644827
10: USER_INFO	DTLS	1081366	1124538944
11: AP_INFO	DTLS	5152	3951584
12: RADIO_INFO	DTLS	266	291560
13: VAP_INFO	DTLS	398	452952
26: FW_APP_CATEGORY	DTLS	2	1784
27: FW_WEB_CC_CATEGORY	DTLS	5	5500
35: PASSIVE_AP_STATION_STATS	DTLS	12543	2865738
36: PASSIVE_CTRL_STA_STATS	DTLS	2156	2153130
42: MCELL_REPORT	DTLS	210661	224143304
45: GEN_DATA	DTLS	3832	4491104
65: STATION_RSSI_INFO_V2	DTLS	232798	247697072
66: AP_NEIGHBORS_V2	DTLS	117511	125031704
67: HWMON_TEMP_DETAIL	DTLS	110	55660
68: HWMON_FAN_DETAIL	DTLS	110	22000
69: HWMON_SENSOR_THRS	DTLS	110	16170
70: HWMON_SENSOR_VAL	DTLS	110	18810
71: HWMON_SYS_INFO	DTLS	110	108020
72: FPAPPS_PORTS_INFO	DTLS	242	29040
73: FPAPPS_PORT_DETAIL	DTLS	1452	1343100
74: FPAPPS_PC_DETAIL_MESSAGE	DTLS	1936	1903088
75: FPAPPS_CTRL_INFO	DTLS	242	22506
76: FPAPPS_CTRL_IP	DTLS	242	19844

Total [27 messages] 6852329 7284995288
(host)[mynode] #show amon-sender stats-counters-all

Id: MsgName NoOfMsgs NoOfRecords
NoOfBytes

0: RADIO_STATS	0	0
0		
1: VAP_STATS	0	0
0		
2: STATION_STATS	0	0
0		
3: AP_NEIGHBORS	0	0
0		

```

4: UNASSOCIATED_STA          0          0
0

5: TAG                        0          0
0

6: SPEC_DEV_DETAILS         0          0
0

7: FW_AGG_SESSIONS          0          0
0

9: FW_APP                    0          0
0
10: USER_INFO                0          0
0
11: AP_INFO                   0          0
0
12: RADIO_INFO                0          0
0
13: VAP_INFO                   0          0
0
14: MON_AP_INFO               0          0
0
15: MON_AP_STATS              0          0
0
16: MON_STA_INFO              0          0
0
17: MON_STA_STATS             0          0
0
18: AP_SYSTEM_STATS           0          0
0

```

Related Commands

Command	Description
<u>clear amon-sender</u>	This command displays AMON sender information.

Command History

Release	Description
ArubaOS 8.8.0.0	The output parameter, TAG of the <code>show amon-sender stats-counters-all</code> command gets incremented when there are RTLS frames from AMON receiver.
ArubaOS 8.4.0.0	The following parameters were added: <code>bundle counters</code> <code>bundle parameters</code> <code>cdt message-type</code>
ArubaOS 8.1.0.0	The following parameters were modified to accept IPv6 address: <code>dest-stats-all</code> <code>dest-stats-inst-0-7</code> <code>interest-table</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show amon source-interface

show amon source-interface

Description

This command displays the source VLAN interface of AMON packets on the controller. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays the source VLAN interface of the AMON feed:

```
(host) [mynode] #show amon source-interface  
amon source-interface:vlan 501
```

Related Commands

Command	Description
amon source-interface	Specifies the IPv4 address of the VLAN as the source IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show ap

```
show ap
  active
  allowed-channels
  allowed-max-EIRP
  am-filter-profile
  analytics
  antenna-status
  ap-cert-mgr
  ap-group
  ap-lacp-striping-ip
  ap-name
  arm
  assoc-throttle-counters
  association
  authorization-profile
  blacklist-clients/denylist-clients
  blacklist-protected/denylist-protected
  blacklist-time/denylist-time
  ble-database
  ble-ibeacon-info
  bss-table
  bw-report
  cellular
  client
  cluster-tech-support
  config
  consolidated-provision
  convert-download-log
  convert-image-list
  convert-setup-image-log
  convert-status
  convert-status-list
  convert-status-summary
  crash-transfer
  database
  database-summary
  debug
  deploy-profile
  details
  dot1x
  enet-link-profile
  essid
  est-status
  general-profile
  get-crash-dumps-status
  global
  greenap
  he-rates
  ht-rates
  image
```


image-preload
ip
license-usage
lldp
load-balancing
mesh
mesh-accesslist-profile
mesh-cluster-profile
mesh-ht-ssid-profile
mesh-radio-profile
mesh-recovery-profile
mfg-image-download-log
mfg-image-setup-image-log
mfg-image-upgrade
mfg-image-upgrade-list
mfg-image-upgrade-status-list
mfg-image-upgrade-status-summary
modem-download-log
modem-upgrade-status
monitor
multizone-profile
owe-tm-info
packet-capture
papi-err
port status
power-mgmt-statistics
profile-usage
provisioning
provisioning-profile
provisioning-rule
provisioning-rules
radio-database
radio-summary
regulatory
regulatory-domain-profile
remote
remote auth-trace-buf
remote blacklist-clients/denylist-clients
remote blacklist-clients-driver/denylist-clients-driver
remote bss-table
remote client status
remote counters
remote debug anul-sta-entries
remote debug association
remote debug association-failure
remote debug bss-config
remote debug bucketmap-counters
remote debug bucketmap datapath
remote debug bucketmap sapd
remote debug bucketmap stm
remote debug client-mgmt-counters
remote debug flash-config
remote debug-mcast-forwarder
remote debug mgmt-frames
remote debug neighbor-cache

remote debug nodelist history
remote-debug-pkt
remote debug sapd
remote debug redun-state history
remote debug sta-msg-stats
remote debug sta-msg-sta-down-entries
remote debug stale_sta
remote debug stm cluster-nodestate
remote debug stm trace-files
remote debug uac-list
remote essid
remote wmm-flow
sapd-debug
snmp
spectrum
spectrum ap-list
spectrum channel-metrics
spectrum channel-summary
spectrum client-list
spectrum debug
spectrum debug fft
spectrum debug monitors
spectrum debug status
spectrum device-duty-cycle
spectrum device-history
spectrum device-summary
spectrum device-list
spectrum device-log
spectrum interference-power
spectrum-load-balancing
spectrum local-override
spectrum monitors
spectrum tech-support
standby
system-profile
tech-support
uac-database
usb-acl-prof
usb-device-mgmt
usb-profile
vht-rates
virtual-beacon-report
vlan-mcast
vlan-usage
wifi-uplink
wifi-uplink blacklist/denylist
wifi-uplink candidates
wifi-uplink connection-history
wifi-uplink connection-trace
wifi-uplink current-profile
wifi-uplink debug
wifi-uplink-profile
wifi-uplink provisioned-profiles
wifi-uplink stats
wifi-uplink status

wifi-uplink neighbors
wired
wired-ap-profile
wired-port-profile
wmm-flow
zigbee-client-database

Description

This command shows the access point settings. Click parameter links to view the corresponding show commands.

Parameter	Description
active	Shows APs currently registered or having clients terminating (in cluster) on this switch.
allowed-channels	Shows the set of allowed channels.
allowed-max-EIRP	Shows max EIRP setting per country per AP type.
analytics recommendations	Shows recommendations received from analytics engine.
antenna-status	Shows operational status of AP antennas.
ap-cert-mgr	Shows contents of /tmp/ap_cert_mgr_debug_log for an AP.
ap-group	Shows contents of AP's group.
ap-lacp-striping-ip	Shows profile to enable/disable AP LACP feature and to specify GRE striping IP to LMS IP mapping.
ap-name	Shows the list of AP names.
arm	Shows ARM Information.
assoc-throttle-counters	Shows counters related to association request throttling.
association	Shows Association table for an AP.
authorization-profile	Shows an AP Authorization profile.
blacklist-clients/denylist-clients	Shows list of clients that have been denied access.

Parameter	Description
<u>blacklist-protected/denylist-protected</u>	Shows all clients that are currently protected against further traffic steering for a period of time.
<u>blacklist-time/denylist-time</u>	Shows the amount of blacklist/denylist time of the STA when it is denylisted in between disconnection and user-timeout.
<u>ble-database</u>	Shows BLE APB information collected by BLE relay.
<u>ble-ibeacon-info</u>	Shows AP's BLE radio iBeacon parameters.
<u>bss-table</u>	Shows BSSIDs of all APs registered on this switch.
<u>bw-report</u>	Shows bandwidth allocation report for an AP.
<u>cellular</u>	Shows cellular information for an AP.
<u>client</u>	Shows wireless client specific information.
<u>cluster-tech-support</u>	Shows cluster information for an AP.
<u>config</u>	Shows AP configuration parameters.
<u>consolidated-provision</u>	Shows consolidated provision details of an AP.
<u>convert-download-log</u>	Shows conversion image downloading logs.
<u>convert-image-list</u>	Shows a list all available images for conversion.
<u>convert-setup-image-log</u>	Shows conversion setup image logs.
<u>convert-status</u>	Shows status of AP image conversion operation.
<u>convert-status-list</u>	Shows only the list of APs and their conversion statuses.
<u>convert-status-summary</u>	Shows status summary of conversion operation.
<u>crash-transfer</u>	Shows info for the AP crash transfer feature, which transfers AP coredump files to the controller flash memory if no dumpserver is configured.
<u>database</u>	Shows list of access points in the database.
<u>database-summary</u>	Shows a general summary of access point information for the controller.

Parameter	Description
<u>debug</u>	Shows debugging information of an AP.
<u>deploy-profile</u>	Shows the ap deploy-profile.
<u>details</u>	Shows details about an AP.
<u>dot1x</u>	Shows details about an 802.1X AP.
<u>enet-link-profile</u>	Shows an AP Ethernet Link profile.
<u>ssid</u>	Shows ESSID Information.
<u>est-status</u>	Shows contents of /tmp/est_status for an AP.
<u>general-profile</u>	Shows the AP general-profile.
<u>get-crash-dumps-status</u>	Shows get crash dumps status.
<u>global</u>	Shows AP's central database.
<u>greenap</u>	Shows details of AP supporting green mode.
<u>he-rates</u>	Shows high-efficiency rate information for a BSS.
<u>ht-rates</u>	Shows high-throughput rate information for a BSS.
<u>image</u>	Shows AP Image version.
<u>image-preload</u>	Shows status of AP image preload operation.
<u>ip</u>	Shows health check IP probe mode.
<u>license-usage</u>	Shows AP license usage information.
<u>lldp</u>	Shows details of Link-layer Discovery Protocol profile.
<u>load-balancing</u>	Shows all BSS where load balancing is enabled.
<u>mesh</u>	Shows all information for a mesh AP.
<u>mesh-accesslist-profile</u>	Shows a mesh access list profile.

Parameter	Description
<u>mesh-cluster-profile</u>	Shows a mesh cluster profile.
<u>mesh-ht-ssid-profile</u>	Shows a mesh High-throughput SSID profile.
<u>mesh-radio-profile</u>	Shows a mesh radio profile.
<u>mesh-recovery-profile</u>	Shows mesh recovery profile information.
<u>monitor</u>	Shows Air Monitor information.
<u>multizone-profile</u>	Shows an AP multizone profile.
<u>owe-tm-info</u>	Shows information about OWE Transition VAPs generated.
<u>packet-capture</u>	Shows packet capture commands.
<u>papi-err</u>	Shows PAPI error messages.
<u>port status</u>	Shows AP wired port information.
<u>power-mgmt-statistics</u>	Shows AP power status statistics.
<u>profile-usage</u>	Shows configuration profiles in use by an AP or a specific BSSID.
<u>provisioning</u>	Shows provisioning parameters currently used by an AP.
<u>provisioning-profile</u>	Shows provisioning profile of an AP.
<u>provisioning-rule</u>	Shows provisioning rule of an AP.
<u>provisioning-rules</u>	Shows provisioning rules of an AP.
<u>radio-database</u>	Shows radio information for APs that are visible to the controller.

Parameter	Description
<u>radio-summary</u>	Shows AP radios currently registered to the controller.
<u>regulatory</u>	Shows regulatory version used by APs.
<u>regulatory-domain-profile</u>	Shows regulatory domain profile of APs.
<u>remote</u>	Shows information from Remote AP.
<u>remote auth-trace-buf</u>	Shows authentication trace buffer on an AP.
<u>remote blacklist-clients/remote denylist-clients</u>	Shows all blacklisted/denylisted clients.
<u>remote blacklist-clients-driver/ remote denylist-cl</u>	Shows all clients blacklisted/denylisted in the driver.
<u>remote bss-table</u>	Shows BSSIDs of all APs registered on the managed device
<u>remote client status</u>	Shows association state of clients.
<u>remote counters</u>	Shows the numbers of message counters for Remote APs.
<u>remote debug anul-sta-entries</u>	Shows a list of VAPs and stations stored in the AP's datapath.
<u>remote debug association</u>	Shows the association table of the AP to identify the clients associated to each AP.
<u>remote debug association-failure</u>	Shows association failure information that can be used to troubleshoot problems on an AP.
<u>remote debug bss-config</u>	Shows the configuration for each BSSID of an AP.
<u>remote debug bucketmap-counters</u>	Shows bucket map counters.
<u>remote debug bucketmap datapath</u>	Shows bucket maps in AP datapath.
<u>remote debug bucketmap sapd</u>	Shows bucket map received from cluster by SAPD process.
<u>remote debug bucketmap stm</u>	Shows bucket map received from cluster by AP STM.
<u>remote debug client-mgmt-counters</u>	Shows the number of each type of message from the clients of an AP.

Parameter	Description
<u>remote debug flash-config</u>	Shows the remote AP configuration stored in flash memory.
<u>remote debug-mcast-forwarder</u>	Shows the Mcast forwarder status for the selected AP.
<u>remote debug mgmt-frames</u>	Shows traced 802.11 management frames for a remote AP.
<u>remote debug neighbor-cache</u>	Shows per-ESSID cached neighbor for a remote AP.
<u>remote debug nodelist history</u>	Shows the cluster node history for a remote AP.
<u>remote-debug-pkt</u>	Shows the packet debugging details of an AP.
<u>remote debug sapd</u>	Shows the state of cluster node in the SAPD process.
<u>remote debug redun-state history</u>	Shows the cluster node history for a remote AP.
<u>remote debug sta-msg-stats</u>	Shows AP-STM to STM message statistics.
<u>remote debug sta-msg-sta-down-entries</u>	Shows STA message for STA Down list.
<u>remote debug stale_sta</u>	Shows information for debugging an AP.
<u>remote debug stm cluster-nodestate</u>	Shows the cluster node state in AP.
<u>remote debug stm trace-files</u>	Shows STM trace files for an AP.
<u>remote debug uac-list</u>	Shows user anchor controller (UAC) list in AP datapath.
<u>remote essid</u>	Shows an ESSID summary for the Managed Device
<u>remote wmm-flow</u>	Shows the Wireless Multimedia (WMM) flows that are active on an AP connected to a Managed Device
<u>sapd-debug log</u>	Shows the SAPD debug log for an AP.
<u>snmp</u>	Shows SNMP tables of APs.
<u>spectrum</u>	Shows spectrum monitor information of APs.
<u>spectrum ap-list</u>	Shows spectrum data seen by an access point that has been converted to a spectrum monitor.

Parameter	Description
<u>spectrum channel-metrics</u>	Shows channel quality, availability, and utilization metrics as seen by a spectrum monitor.
<u>spectrum channel-summary</u>	Shows summary of the 802.11a or 802.11g channels seen by a spectrum monitor.
<u>spectrum client-list</u>	Shows details for clients seen by a specified spectrum monitor.
<u>spectrum debug</u>	Saves spectrum analysis channel information to a file on the spectrum monitor.
<u>spectrum debug fft</u>	Saves Fast Fourier Transform (FFT) power data to a file on the spectrum monitor.
<u>spectrum debug monitors</u>	Shows a detailed description of all spectrum monitors on the controller.
<u>spectrum debug status</u>	Shows detailed status and statistics for a spectrum monitor or hybrid AP.
<u>spectrum device-duty-cycle</u>	Shows the current duty cycle for devices on all channels.
<u>spectrum device-history</u>	Shows the history of the last 256 non- Wi-Fi devices.
<u>spectrum device-log</u>	Shows a time log of add and delete events for non- Wi-Fi devices.
<u>spectrum device-list</u>	Shows a device summary table and channel information for non- Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.
<u>spectrum device-summary</u>	Shows the numbers of Wi-Fi and non- Wi-Fi device types on each channel monitored by a spectrum monitor or hybrid AP.
<u>spectrum interference-power</u>	Shows the interference power detected by a 802.11a or 802.11g radio on a spectrum monitor or hybrid AP.
<u>spectrum tech support</u>	Saves spectrum data for later analysis by technical support.
<u>spectrum-load-balancing</u>	Shows spectrum load balancing information for an AP.
<u>spectrum local-override</u>	Shows a list of AP radios currently converted to spectrum monitors through the spectrum local-override list.

Parameter	Description
<u>spectrum monitors</u>	Shows a list of APs terminating on the controller that are currently configured as spectrum monitors or hybrid APs.
<u>standby</u>	Shows standby APs currently registered on the controller.
<u>system-profile</u>	Shows an AP system profile.
<u>tech-support</u>	Shows all information for an AP that is used by Aruba technical support to diagnose a problem with an AP.
<u>uac-database</u>	Shows User Anchor Controller (UAC) AP database for a cluster.
<u>usb-acl-prof</u>	Shows an AP USB ACL profile.
<u>usb-device-mgmt</u>	Shows the USB devices managed on an AP.
<u>usb-profile</u>	Shows the AP USB profile.
<u>vht-rates</u>	Shows Very-High-Throughput (VHT) rates for an AP that supports 802.11ac.
<u>virtual-beacon-report</u>	Shows the virtual beacon report for an AP or a client with a specific IP or MAC address.
<u>vlan-mcast</u>	Shows user count in each VLAN and timestamps for tunnel to join or leave VLAN-Multicast group.
<u>vlan-usage</u>	Shows the numbers of clients on each VLAN.
<u>wifi-uplink blacklist</u>	Shows a list of Wi-Fi uplink APs that have been denied access.
<u>wifi-uplink candidates</u>	Shows a list of Wi-Fi uplink candidate APs.
<u>wifi-uplink connection-history</u>	Shows the connection history of APs with Wi-Fi uplink.
<u>wifi-uplink connection-trace</u>	Shows the connection trace of APs with Wi-Fi uplink.
<u>wifi-uplink current-profile</u>	Shows the current profile information of APs with Wi-Fi uplink.
<u>wifi-uplink debug</u>	Shows debug information of APs with Wi-Fi uplink.

Parameter	Description
wifi-uplink neighbors	Shows information of neighboring APs by scanning them.
wifi-uplink provisioned-profiles	Shows information of provisioned profiles of APs with Wi-Fi uplink.
wifi-uplink status	Shows the status of APs with Wi-Fi uplink.
wifi-uplink stats	Shows the statistics of APs with Wi-Fi uplink.
wifi-uplink-profile	Shows a list of all Wi-Fi uplink profiles, or display the configuration parameters in a specific Wi-Fi uplink profile.
wired stats	Shows statistics for campus and remote AP wired clients.
wired-ap-profile	Shows a list of all wired AP profiles, or display the configuration parameters in a specific wired AP profile.
wired-port-profile	Shows all AP wired port profiles and their status.
wmm-flow	Shows the Wireless Multimedia (WMM) flow table.
zigbee-client-database	Shows all Zigbee client information of APs.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Config or Enable mode on Mobility Conductor.

show ap active

```
show ap active
  2.4GHz
  5GHz
  6GHz (For ArubaOS 8.9.0.0 or later versions)
  ap-name
  arm-edge
  counters [ap-name <ap-name>] [arm-edge] [dot11a] [dot11g] [ssid <ssid>] [ip-
  addr <ip-addr>] [ip6-addr <ip6-addr>] [type]
  details
  ssid
  ip-addr
  ip6-addr
  type
  voip-only
```

Description

This command shows Access Points registered to a Mobility Conductor. Click parameter links to view the corresponding show commands.

Parameter	Description
2.4GHz	Show 802.11g/2.4 GHz radio information.
5GHz	Show 802.11a/5 GHz radio information.
6GHz (For ArubaOS 8.9.0.0 or later versions)	Show 6 GHz radio information.
ap-name	Shows data for a specified AP name.
arm-edge	Shows the state of ARM edge Access Points.
counters	Shows counters.
details	Shows AP detailed columns.
ssid	Shows data for specified ESSID.
ip-addr	Shows data of an AP for specified IP address.
ip6-addr	Shows data of an AP for specified IPv6 address.
type	Shows information filtered by type of AP.
voip-only	Shows information filtered by associated/active VoIP clients.

Example

The following example shows access points registered to a Mobility Conductor:

```
(host) [mynode] #show ap active

Active AP Table
-----
Name      Group      IP Address      AP Type  Flags  Uptime      Outer IP
Cluster  Role
-----  -
AP345     default    192.168.40.46   345      A2aW   2d:11h:5m:44s  N/A
AP555-0   triradio   192.168.40.2    555      A2at   2d:0h:39m:31s  N/A

Radio 0 Band Ch/EIRP/MaxEIRP/Clients  Radio 1 Band Ch/EIRP/MaxEIRP/Clients
-----
AM                                       AP:5GHz-VHT:44+/10.0/27.2/0
AP:5GHz-HE:40-/10.0/27.7/2            AP:2.4GHz-HE:11/12.0/29.2/0

Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----

AP:5GHz-HE:153/15.0/26.8/0

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:2
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled■ x = Flex Dual Mode 5GHz+2.4GHz

Column	Description
	<ul style="list-style-type: none"> ■ y = Flex Dual Mode 2.4GHz+6GHz ■ z = Flex Dual Mode 5GHz+6GHz
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	New flags, x , y , and z were introduced to indicate the flex dual band support for the AP-615.
ArubaOS 8.9.0.0	The <code>6GHz</code> parameter was introduced for Wi-Fi 6E APs.

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band</code> and <code>Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.


```
show ap active 2GHz <details>
```

Description

This command shows information related to 802.11g radio.

Example

The following example shows 802.11g radio information:

```
(host) [mynode] #show ap active 2.4GHz details

Active AP Table
-----
Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role
Active Clients Standby Clients
Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients
Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----
-----
-----
-----
-----
Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:0
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show ap active 6GHz

show ap active 6GHz <details>

Description

This command shows information related to 6 GHz radio that is active on Wi-Fi 6E APs.

Example

The following example shows 6 GHz radio information.

```
(host) [mynode] (config) #show ap active 6GHz details

Active AP Table
-----
Name      Group      IP Address      AP Type  Flags  Uptime      Outer IP
Cluster Role  Active Clients  Standby Clients  Radio 0 Band
Ch/EIRP/MaxEIRP/Clients  Radio 1 Band Ch/EIRP/MaxEIRP/Clients  Radio 2 Band
Ch/EIRP/MaxEIRP/Clients
-----
-----
-----
-----
hhm-635   hhm-635   10.65.36.220   635     A2a    20d:13h:52m:55s  N/A
              0              0
                                     AP:6GHz-HE:37S/15.0/21.8/0

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
```



```

    A = Enet1 in active/standby mode; B = Battery Boost On; C =
Cellular;
    D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed
802.1x authentication;
    H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing
Enabled; M = Mesh;
    N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
    S = AP connected as standby; X = Maintenance Mode;
    a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u =
Custom-Cert RAP;
    i = Provisioned as Indoor; o = Provisioned as Outdoor;
    p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No
Spectrum FFT support;
    Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t =
Tri-Radio Mode Enabled;
    U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e =
custom EST cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink

Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)

Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC

Num APs:1

```

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none"> ■ 1 = 802.1X authenticated AP ■ 2 = Using IKE version 2; ■ 4 = Using Wi-Fi Uplink ■ A = Enet1 in active/standby mode ■ B = Battery Boost On ■ C = Cellular; ■ D = Disconn. Extra Calls On

Column	Description
	<ul style="list-style-type: none"> ■ E = Wired AP enabled ■ F = AP failed 802.1X authentication ■ H = Hotspot Enabled ■ K = 802.11K Enabled ■ L = Client Balancing Enabled ■ M = Mesh ■ N = 802.11b protection disabled ■ P = PPPOE ■ R = Remote AP ■ S = AP connected as standby ■ X = Maintenance Mode ■ a = Reduce ARP packets in the air ■ d = Drop Mcast/Bcast On ■ u = Custom-Cert RAP ■ i = Provisioned as indoor ■ o = Provisioned as outdoor ■ p = Restriction mode in POE-AF/AT ■ r = 802.11r Enabled ■ t=Tri-radio mode enabled ■ Q = DFS CAC timer running ■ T = Flex Radio Mode is 2.4GHz+5GHz ■ U = Flex Radio Mode is 5GHz ■ V = Flex Radio Mode is 2.4GHz ■ W = Dual 5 GHz Mode Enabled
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Cluster Role	The cluster role of the managed device. The cluster role could be one of the following: <ul style="list-style-type: none"> ■ U = UAC ■ A = AAC ■ SU = Standby UAC ■ SA = Standby AAC
Active Clients	The number of active clients connected to the AP.
Standby Clients	The number of standby clients connected to the AP.
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.

Column	Description
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

```
show ap active ap-name <ap-name>
```

Description

This command shows data for a specified AP name.

Example

The following example shows data for a specified AP name:

```
(host) [mynode] #show ap active ap-name AP-205

Active AP Table
-----
Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role
Active Clients Standby Clients
Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients
Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----
-----
-----
-----
-----
Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:0
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

p = Restriction mode in POE-AF/AT; r = 802.11r Enabled; f = No Spectrum FFT support;
 Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio Mode Enabled;
 U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
 Channel followed by "*" indicates channel selected due to unsupported configured channel.
 "Spectrum" followed by "^" indicates Local Spectrum Override in effect.
 Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz (i.e. 36E+149E)
 Cluster Role: U = UAC, A = AAC, SU = Standby UAC, SA = Standby AAC
 Num APs:0



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none"> ■ 1 = 802.1X authenticated AP ■ 2 = Using IKE version 2; ■ 4 = Using Wi-Fi Uplink ■ A = Enet1 in active/standby mode ■ B = Battery Boost On ■ C = Cellular; ■ D = Disconn. Extra Calls On ■ E = Wired AP enabled ■ F = AP failed 802.1X authentication ■ H = Hotspot Enabled ■ K = 802.11K Enabled ■ L = Client Balancing Enabled ■ M = Mesh ■ N = 802.11b protection disabled ■ P = PPPOE ■ R = Remote AP

Column	Description
	<ul style="list-style-type: none"> ■ S = AP connected as standby ■ X = Maintenance Mode ■ a = Reduce ARP packets in the air ■ d = Drop Mcast/Bcast On ■ u = Custom-Cert RAP ■ i = Provisioned as indoor ■ o = Provisioned as outdoor ■ p = Restriction mode in POE-AF/AT ■ r = 802.11r Enabled ■ t=Tri-radio mode enabled ■ Q = DFS CAC timer running ■ T = Flex Radio Mode is 2.4GHz+5GHz ■ U = Flex Radio Mode is 5GHz ■ V = Flex Radio Mode is 2.4GHz ■ W = Dual 5 GHz Mode Enabled
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band</code> , <code>Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

```
show ap active counters
 2GHz
 5GHz
 ap-name
 arm-edge
 essid
 ip-addr
 ip6-addr
 type
```

Description

This command shows the counters.

Parameter	Description
2GHz	Shows 802.11g radio information.
5GHz	Shows 802.11a radio information.
ap-name	Shows AP information filtered by its name.
arm-edge	Shows the state of ARM edge Access Points.
ssid	Shows data for specified ESSID.
ip-addr	Shows data of an AP for specified IP address.
ip6-addr	Shows data of an AP for specified IPv6 address.
type	Shows information filtered by type of AP.

Example

The following example shows counters:

```
(host)[mynode] #show ap active counters ap-name AP_205
Active AP Table Counters:
Num APs:0
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

```
show ap active essid
```

Description

This command shows data for specified ESSID.

Example

The following example shows data for specified ESSID:

```
(host) [mynode] #show ap active essid First floor

Active AP Table
-----
Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role
Active Clients Standby Clients
Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients
Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----
-----
-----
-----
-----
Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:0
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

```
show ap active ip-addr <ip-addr>
```

Description

This command shows data of an AP for specified IP address.

Example

The following example shows data of an AP for specified IP address:

```
(host) [mynode] #show ap active ip-addr 1.1.1.1

Active AP Table
-----
Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role
Active Clients Standby Clients
Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients
Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----
-----
-----
-----
-----
Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:0
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

```

show ap active type
  access-point[details | 2GHz | 5GHz |voip-only]
  airmatch-monitor [details | 2.4GHz | 5GHz | 6GHz | voip-only]
  air-monitor[details | 2GHz | 5GHz |voip-only]
  ap-monitor[details | 2GHz | 5GHz |voip-only]
  spectrum[details | 2GHz | 5GHz |voip-only]

```

Description

This command shows information filtered by type of AP.

Parameter	Description
access-point	Shows information for Access Points only.
airmatch-monitor	Shows information for AirMatch monitors only.
2.4GHz	Shows 2.4 GHz radio information.
5GHz	Shows 5 GHz radio information.
6GHz	Shows 6 GHz radio information.
details	Shows detailed columns for APs.
voip-only	Shows information filtered by associated/active VoIP clients.
air-monitor	Shows information for Air Monitors only.
ap-monitor	Shows information for AP Monitors only.
spectrum	Shows spectrum sensor information.
details	Shows detailed columns for APs.
2GHz	Shows 802.11g radio information.
5GHz	Shows 802.11a radio information.
voip-only	Shows information filtered by associated/active VoIP clients.

Example

The following example shows information filtered by type of AP:

```
(host) [mynode] #show ap active type access-point details
```

Active AP Table

```
-----  
Name Group IP Address AP Type Flags Uptime Outer IP Cluster Role  
Active Clients Standby Clients  
Radio 0 Band Ch/EIRP/MaxEIRP/Clients Radio 1 Band Ch/EIRP/MaxEIRP/Clients  
Radio 2 Band Ch/EIRP/MaxEIRP/Clients  
-----  
-----  
-----  
Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;  
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;  
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x  
authentication;  
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =  
Mesh;  
N = 802.11b protection disabled; P = PPPOE; R = Remote AP;  
S = AP connected as standby; X = Maintenance Mode;  
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert  
RAP;  
i = Provisioned as Indoor; o = Provisioned as Outdoor;  
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT  
support;  
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio  
Mode Enabled;  
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST  
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink  
Channel followed by "*" indicates channel selected due to unsupported  
configured channel.  
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.  
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz  
(i.e. 36E+149E)  
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC  
Num APs:0
```



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.

Column	Description
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none"> ■ 1 = 802.1X authenticated AP ■ 2 = Using IKE version 2; ■ 4 = Using Wi-Fi Uplink ■ A = Enet1 in active/standby mode ■ B = Battery Boost On ■ C = Cellular; ■ D = Disconn. Extra Calls On ■ E = Wired AP enabled ■ F = AP failed 802.1X authentication ■ H = Hotspot Enabled ■ K = 802.11K Enabled ■ L = Client Balancing Enabled ■ M = Mesh ■ N = 802.11b protection disabled ■ P = PPPOE ■ R = Remote AP ■ S = AP connected as standby ■ X = Maintenance Mode ■ a = Reduce ARP packets in the air ■ d = Drop Mcast/Bcast On ■ u = Custom-Cert RAP ■ i = Provisioned as indoor ■ o = Provisioned as outdoor ■ p = Restriction mode in POE-AF/AT ■ r = 802.11r Enabled ■ t=Tri-radio mode enabled ■ Q = DFS CAC timer running ■ T = Flex Radio Mode is 2.4GHz+5GHz ■ U = Flex Radio Mode is 5GHz ■ V = Flex Radio Mode is 2.4GHz ■ W = Dual 5 GHz Mode Enabled
Uptime	<p>Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i>.</p>
Outer IP	<p>The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).</p>
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	<p>Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.</p>

Column	Description
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>airmatch-monitor</code> parameter was introduced.
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.



In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.
IP address	IP address of the AP, in dotted decimal format.
AP Type	AP model type.
Flags	<p>This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the <code>show ap active</code> command.</p> <ul style="list-style-type: none">■ 1 = 802.1X authenticated AP■ 2 = Using IKE version 2;■ 4 = Using Wi-Fi Uplink■ A = Enet1 in active/standby mode■ B = Battery Boost On■ C = Cellular;■ D = Disconn. Extra Calls On■ E = Wired AP enabled■ F = AP failed 802.1X authentication■ H = Hotspot Enabled■ K = 802.11K Enabled■ L = Client Balancing Enabled■ M = Mesh■ N = 802.11b protection disabled■ P = PPPOE■ R = Remote AP■ S = AP connected as standby■ X = Maintenance Mode■ a = Reduce ARP packets in the air■ d = Drop Mcast/Bcast On■ u = Custom-Cert RAP■ i = Provisioned as indoor■ o = Provisioned as outdoor■ p = Restriction mode in POE-AF/AT■ r = 802.11r Enabled■ t=Tri-radio mode enabled■ Q = DFS CAC timer running■ T = Flex Radio Mode is 2.4GHz+5GHz■ U = Flex Radio Mode is 5GHz■ V = Flex Radio Mode is 2.4GHz■ W = Dual 5 GHz Mode Enabled

Column	Description
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Outer IP	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Conductor. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
Radio 0 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
Radio 1 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> , <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> , and <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> will include the following details: <ul style="list-style-type: none"> ■ MPP: Indicates mesh enabled radio of a mesh portal. ■ MPC: The mesh point radio that has a parent link. ■ MPA: The mesh point radio without a parent link.
ArubaOS 8.6.0.0	Two new output parameters <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and <code>flag t</code> were introduced.

Release	Modification
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.3.0.0	New flags, T , U , V , and W were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show ap-group

```
show ap-group [default|NoAuthApGroup|<profile-name>]
```

Description

This command shows configuration for an AP group. Run this command without the optional parameters to display the entire AP group list, including profile status for each profile. Include an AP group name to display detailed configuration for that AP group.

Parameter	Description
default	Shows setting for default AP group.
NoAuthApGroup	Shows setting for NoAuthAP group.
<profile-name>	Shows setting for specified AP group.

Examples

The following example shows the AP group list:

```
(host) [mynode] #show ap-group

AP group List
-----
Name           Profile Status
----           -
default
NoAuthApGroup  Predefined (changed)

Total:2
```

The following example shows the configuration of an AP group named **default**:

```
(host) [mynode] #show ap-group default

AP group "default"
-----
Parameter                               Value      Set
-----
Virtual AP                               N/A
802.11a radio profile                    default
802.11g radio profile                    default
802.11 6GHz radio profile                default
802.11 60GHz radio profile               default
Ethernet interface 0 port configuration  default
Ethernet interface 1 port configuration  default
```

```

Ethernet interface 2 port configuration shutdown
Ethernet interface 3 port configuration shutdown
Ethernet interface 4 port configuration shutdown
Ethernet usb port configuration shutdown
AP system profile default
AP multizone profile default
802.11a Traffic Management profile N/A
802.11g Traffic Management profile N/A
Regulatory Domain profile default
RF Optimization profile default
RF Event Thresholds profile default
IDS profile default
Mesh Radio profile default
Mesh Cluster profile N/A
AM filter profile default
Provisioning profile N/A
AP authorization profile N/A
Mesh Accesslist profile ACL
Airslice profile Airslice profile 1

```

The output of this command includes the following parameters:

Parameter	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP group.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP group.
802.11 6GHz radio profile	Profile that defines 802.11 6 GHz radio settings for the AP group.
802.11 60GHz radio profile	Profile that defines 802.11 60 GHz radio settings for the AP group.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP group.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP group.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.

Parameter	Description
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP group.
Regulatory Domain profile	Name of the regulatory domain profile for the AP group.
SNMP profile	Name of the SNMP profile for the AP group.
RF Optimization profile	Name of the RF optimization profile for the AP group.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP group.
IDS profile	IDS profile for the AP group.
Mesh Radio profile	Mesh radio profile assigned to the AP group.
Mesh Cluster profile	Mesh cluster profile assigned to the AP group.
Mesh Accesslist Profile	Mesh access list profile assigned to the AP.
AirSlice Profile	Air Slice profile assigned to the AP.

Related Commands

Command	Description
ap-group	This command configures an AP group.

Command History

Release	Modification
ArubaOS 8.9.0.0	The output was modified to include the 802.11 6GHz radio profile parameter.
ArubaOS 8.7.0.0	The output was modified to include the following parameters: <ul style="list-style-type: none"> ■ Mesh Accesslist Profile ■ AirSlice Profile
ArubaOS 8.5.0.0	The output of this command was modified to display the Ethernet usb port configuration parameter and its corresponding value.

Release	Modification
ArubaOS 8.4.0.0	The output of this command was modified to display the <code>802.11 60GHz radio profile</code> parameter and its corresponding value.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap-name

```
show ap-name [<profile-name>]
```

Description

This command shows the list of AP names. Run this command without the optional parameter to show the list of AP names. Include <profile-name> to show detailed configuration information for that AP name.

Parameter	Description
[<profile-name>]	Shows detailed configuration information for the specified AP name.

Examples

The following example shows the AP name list:

```
(host) [mynode] #show ap-name

AP name List
-----
Name  Profile Status
----  -
corp1

Total:1
```

The following example shows the configuration settings for an AP named corp1:

```
(host) [mynode] #show ap-name corp1

AP name "corp1"
-----
Parameter                               Value
-----
Virtual AP                               N/A
802.11a radio profile                     default
802.11g radio profile                     default
Ethernet interface 0 port configuration   default
Ethernet interface 1 port configuration   default
Ethernet interface 2 port configuration   shutdown
Ethernet interface 3 port configuration   shutdown
Ethernet interface 4 port configuration   shutdown
AP system profile                         default
AP multizone profile                      default
802.11a Traffic Management profile        N/A
```

802.11g Traffic Management profile	N/A
Regulatory Domain profile	default
RF Optimization profile	default
RF Event Thresholds profile	default
IDS profile	default
Mesh Radio profile	default
Mesh Cluster profile	N/A
AM filter profile	default
Provisioning profile	N/A
AP authorization profile	N/A
Mesh Accesslist profile	ACL
Airslice profile	Airslice profile 1

The output of this command includes the following parameters:

Column	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
Excluded Virtual AP	Excludes the specified mesh cluster profile from this AP.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP.
Regulatory Domain profile	Name of the regulatory domain profile for the AP.
RF Optimization profile	Name of the RF optimization profile for the AP.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP.
IDS profile	IDS profile for the AP.

Column	Description
Mesh Radio profile	Mesh radio profile assigned to the AP.
Mesh Cluster profile	Mesh cluster profile assigned to the AP.
Excluded Mesh Cluster profile	Excludes the specified mesh cluster profile from this AP.
Mesh Accesslist Profile	Mesh access list profile assigned to the AP.
AirSlice Profile	Air Slice profile assigned to the AP.

Related Commands

Command	Description
<code>ap-name</code>	This command configures a specific AP.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output was modified to include the following parameters: <ul style="list-style-type: none"> ■ Mesh Accesslist Profile ■ AirSlice Profile
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap allowed-channels

```
show ap allowed-channels
  ap-name <ap-name>
  country-code <country-code> [ap-type <ap-type>]
  ip-addr <ip-addr>
```

Description

This command shows the allowed channels on a specific AP name, country code, or IP address. Specify the country code for your controller during initial setup. Changing the country code causes the valid channel lists to be reset to the defaults for that country.

Parameter	Description
ap-name <ap-name>	Specifies name of an AP.
country-code <country-code> [ap-type <ap-type>]	Specifies country code. If you specify the optional ap-type <ap-type> parameter, the output shows allowed channels for the specified AP type in that country code. The <ap-type> parameter is the two or three digit model number of the AP, such as 135 for AP-135 or 225 for AP-225. For remote APs, like RAP-3WN, specify the prefix RAP- before the AP model number. If the AP model number includes an alphabetic suffix, such as the AP-175AC, specify the suffix after the model number. Note that the suffix may be case-sensitive.
<ip-addr>	Specifies the IP address of an AP.

Examples

The following example shows all allowed channels for the country code **US**.

- For versions prior to ArubaOS 8.9.0.0:

```
(host) [mynode]# show ap allowed-channels US

Allowed Channels for Country Code "US" Country "United States"
-----
PHY Type                Allowed Channels
-----
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 120 124
128 132 136 140 144 149 153 157 161 165
802.11g (outdoor)       1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)       36 40 44 48 52 56 60 64 100 104 108 112 116 120 124
```

```

128 132 136 140 144 149 153 157 161 165
802.11g 40MHz (indoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor) 36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
802.11g 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor) 36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
802.11a 80MHz (indoor) 36-48 52-64 100-112 116-128 132-144 149-161
802.11a 80MHz (outdoor) 36-48 52-64 100-112 116-128 132-144 149-161
802.11a (DFS) 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144

```

■ ArubaOS 8.9.0.0 or later versions:

```

(host) [mynode]# show ap allowed-channels country-code US

Allowed Channels for Country Code "US" Country "United States"
-----
PHY Type                Allowed Channels
-----
2.4GHz (indoor)         1 2 3 4 5 6 7 8 9 10 11
5GHz (indoor)           36 40 44 48 52 56 60 64 100 104 108 112 116 120 124
128 132 136 140 144 149 153 157 161 165
6GHz (LP indoor)       1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69
73 77 81 85 89 93 97 101 105 109 113 117 121 125 129 133 137 141 145 149 153
157 161 165 169 173 177 181 185 189 193 197 201 205 209 213 217 221 225 229
233
2.4GHz (outdoor)       1 2 3 4 5 6 7 8 9 10 11
5GHz (outdoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 120 124
128 132 136 140 144 149 153 157 161 165
6GHz (outdoor)         1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69
73 77 81 85 89 93 121 125 129 133 137 141 145 149 153 157 161 165 169 173
177 181 185
2.4GHz 40MHz (indoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
5GHz 40MHz (indoor)    36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
6GHz 40MHz (LP indoor) 1-5 9-13 17-21 25-29 33-37 41-45 49-53 57-61 65-69
73-77 81-85 89-93 97-101 105-109 113-117 121-125 129-133 137-141 145-149
153-157 161-165 169-173 177-181 185-189 193-197 201-205 209-213 217-221 225-
229
2.4GHz 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
5GHz 40MHz (outdoor) 36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
6GHz 40MHz (outdoor) 1-5 9-13 17-21 25-29 33-37 41-45 49-53 57-61 65-69
73-77 81-85 89-93 121-125 129-133 137-141 145-149 153-157 161-165 169-173
177-181
5GHz 80MHz (indoor)    36-48 52-64 100-112 116-128 132-144 149-161
5GHz 80MHz (outdoor) 36-48 52-64 100-112 116-128 132-144 149-161
6GHz 80MHz (LP indoor) 1-13 17-29 33-45 49-61 65-77 81-93 97-109 113-125
129-141 145-157 161-173 177-189 193-205 209-221
6GHz 80MHz (outdoor) 1-13 17-29 33-45 49-61 65-77 81-93 129-141 145-157
161-173
5GHz 160MHz (indoor) 36-64 100-128
5GHz 160MHz (outdoor) 36-64 100-128

```

```

6GHz 160MHz (LP indoor) 1-29 33-61 65-93 97-125 129-157 161-189 193-221
6GHz 160MHz (outdoor) 1-29 33-61 65-93 129-157
5GHz (DFS) 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144

```

Related Commands

Command	Description
ap regulatory activate	This command activates the specified regulatory certificate.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the following: <ul style="list-style-type: none"> Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values respectively under PHY Type parameter. Added 6Ghz value under <code>PHY Type</code> parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap allowed-max-eirp

```
show ap allowed-max-EIRP {ap-name <ap-name>}|{ip-addr <ip-addr>}
```

Description

The output of this command shows the regulatory power limits per channel for a specified AP. The values showed in the output of this command include the antenna gain for that device, regardless of whether the AP antenna is internal or external. MIMO gain (if applicable) is also accounted for in the maximum EIRP limits.

Parameter	Description
ap-name <ap-name>	Shows the maximum EIRP setting per country per AP type for specified AP name.
ip-addr <ip-addr>	Shows the maximum EIRP setting per country per AP type for specified IP address.

Examples

The output of this example shows the allowed per-channel EIRP maximums for an AP-325. In the following example, the output is divided into two parts to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
(host)# show ap allowed-max-eirp ap-name local-ap-325

Max EIRP setting for AP-325
-----
Channel 1  2  3  4  5  6  7  8  9  10 11 12 13 14 36 40 44
48 52 56 60
-----
-- -- -- --
b      19 19 19 19 19 19 19 19 19 19 19 19 19 * * * *
* * * *
g/a    19 19 19 19 19 19 19 19 19 19 19 19 19 * 22 22 22
22 22 22 22
HT 20  19 19 19 19 19 19 19 19 19 19 19 19 * 22 22 22
22 22 22 22
HT 40  19 19 19 19 19 19 19 19 19 19 19 19 * 22 22 22
22 22 22 22
VHT 80  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *  *
22 22 22 22

64 100 104 108 112 116 120 124 128 132 136 140 144 149 153
157 161 16
-----
-  ---  ---
-  ---  ---
```

*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
	*	*														
22	*	*	*	*	*	*	*	*	*	*	*	*	*	22	22	22
	22	22														
22	*	*	*	*	*	*	*	*	*	*	*	*	*	22	22	22
	22	22														
22	*	*	*	*	*	*	*	*	*	*	*	*	*	22	22	22
	22	22														
22	*	*	*	*	*	*	*	*	*	*	*	*	*	22	22	22
	22	22														

Related Commands

Command	Description
ap regulatory activate	This command activates the specified regulatory certificate.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap am-filter-profile

```
show ap am-filter-profile
  default
  <profile-name>
```

Description

This command shows the AM filter for an AP.

Parameter	Description
<profile-name>	Shows AM filter for specified profile name.

Example

The following example shows the AM filter for an AP:

```
(host) [mynode] #show ap am-filter-profile

AM Filter List
-----
Name      References  Profile Status
----      -
default  2

Total:1
The following example shows the AM filter for a default AP:
(host) [mynode] #show ap am-filter-profile default

AM Filter "default"
-----
Parameter                Value      Set
-----                -
Filtering                 Disabled
Allow AP's Group         Disabled
Allow Frames from Self   Disabled
Allowed AP Group         N/A
Allowed AP                N/A
```

Related Commands

Command	Description
ap am-filter-profile	This command configures an AM filter.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap analytics recommendations

ap-setting
pending-ap
radio-setting
stats

Description

This command shows the recommendations received from an analytics engine. This information includes the EIRP recommendations, channel-bandwidth recommendations, and regulatory domain profile recommendations to an AP. Click parameter links to view the corresponding show commands.

Parameter	Description
ap-setting	Displays the recommendations for AP level settings.
pending-ap	Displays the pending AP list.
radio-setting	Displays the recommendations for an active AP.
stats	Displays the statistics for recommendations received by the analytics engine.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap analytics recommendations ap-setting

```
database <all|ap-name|inactive|invalid|ip-addr|ip6-addr|valid|wired-mac>  
running <all|ap-name|ip-addr|ip6-addr|wired-mac>
```

Description

This command shows the recommendations for AP level settings.

Parameter	Description
database	Displays the recommendations available in the database.
all	Displays all the recommendations available in the database.
ap-name	Displays the recommendations available for an AP in the database.
inactive	Displays all the recommendation entries for inactive AP(s) in database.
invalid	Displays invalid recommendation entries in database.
ip-addr	Displays the recommendations available for an IP address of the AP .
ip6-addr	Displays the recommendations available for an IPv6 address of the AP.
valid	Displays valid recommendation entries in database.
wired-mac	Displays the recommendations available for a MAC address of the AP.
running	Displays all the recommendation entries for active AP(s) in database.
all	Displays all the recommendations available in the database.
ap-name	Displays the recommendations available for an AP in the database.
ip-addr	Displays the recommendations available for an IP address of the AP .
ip6-addr	Displays the recommendations available for an IPv6 address of the AP.
wired-mac	Displays the recommendations available for a MAC address of the AP.

Example

The following example shows the AP analytics recommendations data:

```
(host) [mynode] #show ap analytics recommendations ap-setting database all
AP Recommendations Info
```

```
-----
Wired-MAC AP Name Assign source 2.4GHz 20MHz Channels 2.4GHz 40MHz
Channels 5GHz 20MHz Channels 5GHz 40MHz Channels
5GHz 80MHz Channels 5GHz 160MHz Channels Version Last Failed Version
Failure Reason
```

```
-----
-----
-----
-----
-----
Total count :0
```

```
(host) [mynode] #show ap analytics recommendations ap-setting running all
AP Recommendations Info
```

```
-----
Wired-MAC AP Name Assign source Version id 2.4GHz 20MHz Channels 2.4GHz
40MHz Channels 5GHz 20MHz Channels 5GHz 40MHz Channels
5GHz 80MHz Channels 5GHz 160MHz Channels
```

```
-----
-----
-----
-----
-----
Total count :0
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```
all
ip-addr
ip6-addr
```

Description

This command displays the pending AP list.

Parameter	Description
all	Displays all the recommendations available in the database.
ip-addr	Displays the recommendations available for an IP address of the AP .
ip6-addr	Displays the recommendations available for an IPv6 address of the AP.

Example

The following example shows the AP analytics recommendations data:

```
(host)[mynode] #show ap analytics recommendations pending-ap all
MD Recommendations pending Info
-----
MD IP   AP Name
-----
Total count :0
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.


```
database <all|ap-name|inactive|invalid|ip-addr|ip6-addr|valid|wired-mac>  
running <all|ap-name|ip-addr|ip6-addr|wired-mac>
```

Description

This command shows the recommendations for radio level settings.

Parameter	Description
database	Displays the recommendations available in the database.
all	Displays all the recommendations available in the database.
ap-name	Displays the recommendations available for an AP in the database.
inactive	Displays all the recommendation entries for inactive AP(s) in database.
invalid	Displays invalid recommendation entries in database.
ip-addr	Displays the recommendations available for an IP address of the AP .
ip6-addr	Displays the recommendations available for an IPv6 address of the AP.
valid	Displays valid recommendation entries in database.
wired-mac	Displays the recommendations available for a MAC address of the AP.
running	Displays all the recommendation entries for active AP(s) in database.
all	Displays all the recommendations available in the database.
ap-name	Displays the recommendations available for an AP in the database.
ip-addr	Displays the recommendations available for an IP address of the AP .
ip6-addr	Displays the recommendations available for an IPv6 address of the AP.
wired-mac	Displays the recommendations available for a MAC address of the AP.


```
all
last
```

Description

Displays the statistics for recommendations received by the analytics engine.

Parameter	Description
all	Displays all the statistics recommendation entries.
last	Displays specific count of latest statistics recommendation entries.

Example

The following example shows all the statistics recommendation entries:

```
(host)[mynode] #show ap analytics recommendations stats all
Flags: B - Channel Bandwidth | C - Channel-list | E - EIRP
Analytics Statistics
-----
ID  Timestamp  Rules-Filename  Schema Version Major/Minor/Patch  Analytics
ID  Revoke All/Radio/AP  Total  Processed E/B/C  Total Error E/B/C
--  -----
-  -----
Total count :0
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```
show ap antenna status
```

```
ap-name <name> radio <0,1,2> advanced
ip-addr <ip-address> radio <0,1,2> advanced
ip6-addr <ipv6-address> radio <0,1,2> advanced
```

Description

This command displays the operational antenna status of APs, and helps in identifying malfunctioning antennas. The status is displayed by comparing the SNR values received on each antenna.

Parameter	Description
ap-name <ap-name>	Name of the access point.
ip-addr <ip-addr>	IP address of the access point.
ip6-addr <ip-addr>	IPv6 address of the access point.
radio	Radio ID (0,1 or 2)
advanced	Use this optional parameter to view additional statistics.

The command displays the following status:

Status	Description
OK	Antenna is fine.
NOT_OK	Antenna is either loose or malfunctioning.
PENDING	The status of the antenna is yet to be determined.

Example

The following example displays the operational antenna status of an APs:

```
(host) [mynode] #show ap antenna-status ap-name SSAP335 radio 1 advanced
Antenna Status
-----
#Chains    Avg Rx SNR  Status
-----
0          0          PENDING
1          0          PENDING
```

```
2          0          PENDING
3          0          PENDING
```

```
DEBUG
```

```
LAST 10 AVG_SNR values:
```

```
Chain[0]: N/A
```

```
Chain[1]: N/A
```

```
Chain[2]: N/A
```

```
Chain[3]: N/A
```

```
DEBUG
```

```
LAST 10 ANTENNA CHECKS: (0-PASS 1-FAIL)
```

```
Chain[0]: N/A
```

```
Chain[1]: N/A
```

```
Chain[2]: N/A
```

```
Chain[3]: N/A
```

Related Commands

Command	Description
show ap provisioning	This command shows the provisioning parameters currently used by an AP.

Command History

Revision	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap ap-cert-mgr

```
show ap ap-cert-mgr
log {ap-name <ap-name>[<page>]|ip-addr <ip-addr>[<page>]}
```

Description

This command displays the contents of the debug log file for an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
log	Show debug log for an AP.
ap-name <ap-name> ip-addr <ip-addr>	Specify name or IP address of the AP .
<page>	Specify page number of the log file.

Example

The following command displays the debug logs for an AP.

```
(host) [mynode] ##show ap ap-cert-mgr log ip-addr 192.168.1.25
```

Related Commands

Command	Description
show ap debug	This command displays the AP debugging information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap ap-group

```
show ap ap-group {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip-addr>|wired-mac <mac-addr>}
```

Description

Shows the AP group settings for an individual AP. Use this command to display the contents of an AP's group profile. If you know the name of the group whose profile settings you want to view, use the command `show ap-group <profile-name>`. To view a list of all configured AP groups on your Mobility Conductor, use the command `show ap-group`.

Parameter	Description
ap-name <ap-name>	Shows data for an AP with a specific name.
bssid <bssid>	Shows data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.
ip6-addr <ip-addr>	Shows data for an AP with a specific IPv6 address.
wired-mac <mac-addr>	Shows data for an AP with a specific MAC address.

Examples

In the example below, the output of this command lists the profiles associated with the AP group **Corp13**.

```
(host) [mynode] #show ap ap-group AP2

AP group "corp13"
-----
Parameter                               Value
-----
Virtual AP                               N/A
802.11a radio profile                     default
802.11g radio profile                     default
Ethernet interface 0 port configuration   default
Ethernet interface 1 port configuration   default
Ethernet interface 2 port configuration   shutdown
Ethernet interface 3 port configuration   shutdown
Ethernet interface 4 port configuration   shutdown
AP system profile                         default
AP multizone profile                       default
802.11a Traffic Management profile         N/A
```


802.11g Traffic Management profile	N/A
Regulatory Domain profile	default
RF Optimization profile	default
RF Event Thresholds profile	default
IDS profile	default
Mesh Radio profile	default
Mesh Cluster profile	N/A
AM filter profile	default
Provisioning profile	N/A
AP authorization profile	N/A

Related Commands

Command	Description
ap-group	Configure your AP groups and AP group profiles.

Command History

Revision	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```

show ap arm
  bandwidth management
  client-match debug state
  client-match history
  client-match mapping
  client-match msg-stats
  client-match neighbors
  client-match pending
  client-match probe-report
  client-match radio-summary
  client-match restriction-table
  client-match rules
  client-match summary
  client-match unsupported
  history
  neighbors
  rf-summary
  scan-times
  split-scan-history
  state
  status
  virtual-beacon-report

```

Description

This command displays ARM information. Click parameter links to view the corresponding show commands.

Parameter	Description
bandwidth management	Shows bandwidth management information for clients associated to an AP.
client-match debug state	Shows the debug information for internal state of objects.
client-match history	Shows the history of AP association changes triggered by the ClientMatch feature.
client-match mapping	Shows the mapping of radio to envID.
client-match msg-stats	Shows Client Match related message stats.
client-match neighbors	Shows the BSSID of other APs seen by clients in the select AP's RF neighborhood.
client-match pending	Shows the pending moves.
client-match probe-report	Shows the client probe report for the specified AP.

Parameter	Description
client-match radio-summary	Shows the summary of radios in the network.
client-match restriction-table	Shows the list of clients that ClientMatch has restricted from the specified AP.
client-match rules	Shows the rules of AP association changes triggered by the client match feature.
client-match summary	Shows the history of AP association changes triggered by the client match feature.
client-match unsupported	Shows a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
history	Shows the history of the channel and power changes due to Adaptive Radio Management (ARM).
neighbors	Shows the ARM settings for an AP's neighbors.
rf-summary	Shows the state and statistics for all channels being monitored by an individual AP.
scan-times	Shows channel scan times for an individual AP and information on the channel being scanned.
split-scan-history	Show scanning information for a "split-scan".
state	Shows aggregate ARM neighbor information.
status	Show the status of ARM on AP.
virtual-beacon-report	Shows the virtual beacon report for an AP

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on managed devices.

show ap arm bandwidth-management

```
show ap arm bandwidth-management ap-name <ap-name> ip-addr <ip-addr>
```

Description

If the client match feature is enabled, the output of this command shows bandwidth management information for clients associated to an AP.

Parameter	Description
ap-name <ap-name>	Name of the access point.
ip-addr <ip-addr>	IP address of the access point.

Example

The following command shows bandwidth management information for clients associated to an AP,

```
(host) [md] #show ap arm bandwidth-management ap-name AP-225
Interface :wifi0
Shaping policy:Default-access (no stats)
Interface :wifi1
Shaping policy:Default-access (no stats)
```

Related Commands

Command	Description
aaa bandwidth-contract	This command configures a bandwidth contract.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Managed Device.

show ap arm client-match debug state

```
show ap arm client-match debug state  
{bssid <bssid>|client-mac <client-mac>|radio-bssid <radio-bssid>}
```

Description

If the Client Match feature is enabled, the output of this command displays the debug information for internal state of objects. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
bssid <bssid>	The BSSID for VAPs.
client-mac <client-mac>	The MAC address for stations.
radio-bssid <radio-bssid>	The BSSID for radios.

Example

```
(host)#show ap arm client-match debug state bssid 90:4c:81:73:d8:b0  
Mac :90:4c:81:cf:3d:8a  
BSSID :90:4c:81:73:d8:b0  
Radio BSSID :90:4c:81:73:d8:b0  
ESSID :S15_ClientMatch  
Eth Mac :90:4c:81:cf:3d:8a  
Name :AP515  
11k/11r/11h/WMM/UAPSD/HT/VHT/HE:0/0/1/1/1/1/1/1  
First Sap/ Dummy :1/0  
Radio:0x0x7fce400075e0  
VHT Cap Info/ MUMIMO/ CHA:0x38001b1/0/0
```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.

Command	Description
<u>show ap arm client-match neighbors</u>	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match history

```
show ap arm client-match history
  advanced
  client-mac <macaddr>
```

Description

If the ClientMatch feature is enabled, the output of this command shows the history of AP association changes triggered by the ClientMatch feature.

Parameter	Description
advanced	Provides additional client-match history information, including: <ul style="list-style-type: none">▪ Eff_Signal▪ EIRP▪ ESSID
client-mac <macaddr>	MAC address of a client for which you want to view a history of AP association changes triggered by the client match feature.

Example

The following command displays information on the ClientMatch history:

```
(AP-7010) # show ap arm client-match history

S: Source, T: Target, A: Actual , As: Actual Assoc req sig
BTM-ACC: 11v BTM Accept, BTM-REJ#: 11v-BTM Reject with reason #, BTM-TO:
11v-BTM Timeout, BTM-FA: 11v-BTM False Accept
Unit of Roam Time: second
Unit of Signal: dBm

ARM Client match History
-----
Time of Change Station Reason Status/Roam Time/Mode Signal(S/T/A/As) Band
(S/T/A) Radio Bssid(S/T/A) AP Name(S/T/A)
-----
-----
2019-12-16 17:04:15 48:e2:44:b1:8a:95 User-action Success/1/BTM-ACC -45/-
43/-43/-40 5G/5G/5G
9c:8c:d8:12:81:10/80:8d:b7:80:ad:40/80:8d:b7:80:ad:40 AP515-Desk-1/AP555-2-
1/AP555-2-1
2019-12-16 16:58:32 48:e2:44:b1:2c:e3 User-action Success/1/BTM-ACC -49/-
44/-44/-39 5G/5G/5G
9c:8c:d8:12:81:10/80:8d:b7:80:ad:40/80:8d:b7:80:ad:40 AP515-Desk-1/AP555-2-
1/AP555-2-1
```


The output of this command includes the following parameters:

Column	Description
Time of Change	Timestamp showing the date and time the client match feature associated the client to a different AP radio.
Station	The station MAC address.
Reason	<p>Reason why the client match feature made the change. Possible reasons include:</p> <ul style="list-style-type: none"> ■ Sticky: A mobile roaming client was staying associated (sticking) to a sub-optimal AP for too long. ■ Band steer: A dual-band capable client was steered toward a 5Ghz radio on a dual-band AP. ■ Band Balance: A dual-band capable client was steered toward a different radio to balance the load between the two radios on a single AP. ■ Load Balance: Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected from each underutilized AP. ■ MU-Steer: A MU-MIMO capable client was steered to a MU-MIMO capable AP. ■ HE-Steer: A HE capable client was steered to a HE capable AP on the same band.
Status/Roam Time/Mode	The status, roam time, and mode of client steering using Client Match.
Signal (S/T/A/As)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: Radio signal strength of the source AP ■ T: Radio signal strength of the target AP ■ A: Radio signal strength of the AP that the client is actually associated to ■ AS : Radio signal strength of the target AP at steer completion
Band (S/T/A)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: Radio frequency band of the source AP (e.g. 2.4GHz and 5GHz) ■ T: Radio frequency band of the target AP ■ A: Radio frequency band of the AP that the client is actually associated to
Radio BSSID (S/T/A)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: MAC address of the source AP radio ■ T: MAC address of the target AP radio ■ A: MAC address of the AP radio that the client is actually associated to
AP Name (S/T/A)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: Name of the source AP ■ T: Name of the target AP

Column	Description
	<ul style="list-style-type: none"> ■ A: Name of the AP that the client is actually associated to

The advanced command provides additional information on the Client Match history.

```
(host) #show ap arm client-match history advanced

S: Source, T: Target, A: Actual, As: Actual Assoc req sig
Unit of Roam Time: second
Unit of Eff_Signal, Signal, EIRP: dBm

ARM Client match History
-----
Time of Change      Station           Reason           Status/Roam Time  Eff_
Signal(S/T/A/As)   Signal(S/T/A/As) EIRP(S/T/A)      Band(S/T/A)
Radio Bssid(S/T/A)                               AP Name(S/T/A)
Essid(S/A)
-----
-----
-----
2014-05-13 16:30:08 f8:f1:b6:03:0d:ff Band-steer      Success/1      -
35/-50/-50         -35/-50/-50     21/21/21        2.4G/5G/5G
6c:f3:7f:e7:2d:40/6c:f3:7f:e7:2d:50/6c:f3:7f:e7:2d:50 ap225/ap225/ap225
jxie2/jxie2
```

The output of this command includes the following additional parameters:

Column	Description
Eff_Signal (S/T/A)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: The relative received signal strength indicator (RSSI) of the source AP radio. This value is derived from the transmit power of the source AP radio and received power from the client. ■ T: The relative RSSI of the target AP radio. This value is derived from the transmit power of the target AP radio and received power from the client. ■ A: The relative RSSI of the AP radio that the client is actually associated to. This value is derived from the transmit power of the AP radio and received power from the client.
EIRP (S/T/A)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ S: The amount of power transmitted from an antennae in the source AP ■ T: The amount of power transmitted from an antennae in the target AP ■ A: The amount of power transmitted from an antennae in the AP that the client is actually associated to

Column	Description
Essid (S/A)	The output of this column shows the following values: <ul style="list-style-type: none"> ■ S: The identifying name of the source wireless network ■ A: The identifying name of the wireless network the client is actually associated to

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match restriction-table	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output of the command was modified to display information on clients having only IPv4 or IPv6 address, or a combination of both.
ArubaOS 8.3.0.0	A new output value, AS was introduced for the Signal output column.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match mapping

show ap arm client-match mapping

Description

If the client match feature is enabled, the output of this command shows the mapping of radio to envID.

Example

The following command displays the mapping of radio to envID,

```
(host)[mm] #show ap arm client-match mapping
Client Match Mapping
-----
Radio BSSID  Env ID
-----
```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match restriction-table	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```
show ap arm client-match msg-stats
  radio <radio-bssid>
```

Description

If the Client Match feature is enabled, the output of this command displays Client Match related message stats. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
radio <radio-bssid>	The BSSID of the radio.

Example

```
(host) #show ap arm client-match msg-stats
ARM PAPI in pkt statistics -
ARM update :: 0
Dropped :: 0
Trigger Client Assist :: 0
Client Match Report :: 0
802.11k Action Frame :: 0
802.11v Action Frame :: 0
CM VBR Report :: 0
Client Management Message :: 0
802.11 Management Message :: 0
ARM RBCM Activation Message :: 0
ARM PAPI out pkt statistics -
ARM update :: 0
Dropped :: 0
Trigger Client Assist :: 0
Client Match Report :: 0
802.11k Action Frame :: 0
802.11v Action Frame :: 0
CM VBR Report :: 0
Client Management Message :: 0
802.11 Management Message :: 0
ARM RBCM Activation Message :: 0
```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match restriction-table	This command displays the list of clients that ClientMatch has restricted from the specified AP.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match neighbors

```
show ap arm client-match neighbors
  ap-name <name>
  ip-addr <ipaddr>
  ip6-addr <ipaddr>
```

Description

If the client match feature is enabled, the output of this command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Parameter	Description
ap-name <name>	View neighboring clients for an AP with a specified name
ip-addr <ipaddr>	View neighboring clients for an AP with a specified IP address.
ipv6-addr <ipaddr>	View neighboring clients for an AP with a specified IPv6 address.

Example

```
(host) [mynode] #show ap arm client-match neighbors ap-name 345-9C
Client View
-----
AP      BSSID                Channel  Clients
--      -
345-9C  c8:b5:ad:ba:f9:d0    157     1
334-12  18:64:72:7e:e1:30    44      0
345-9C  c8:b5:ad:ba:f9:c0    6       0
```

The output of this command includes the following parameters:

Parameter	Description
BSSID	BSSID of the AP.
Channel	Channel of operation of the AP.
Clients	Total number of clients.

Related Commands

Command	Description
<u>rf arm-profile</u>	This command enables ClientMatch.
<u>show ap arm client-match probe-report</u>	This command displays the client probe report for the specified AP.
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match pending

```
show ap arm client-match pending
```

Description

If the Client Match feature is enabled, the output of this command displays the pending moves. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Example

```
(host)#show ap arm client-match pending
S: Source, T: Target, A: Actual , As: Actual Assoc req sig
BTM-ACC: 11v BTM Accept, BTM-REJ#: 11v-BTM Reject with reason #, BTM-TO:
11v-BTM Timeout, BTM-FA: 11v-BTM False Accept
Unit of Roam Time: second
Unit of Signal: dBm
ARM Client match History
-----
Time of Change  Station  Reason  Status/Roam Time/Mode  Signal(S/T/A/As)
Band(S/T/A)   Radio  Bssid(S/T/A)  AP Name(S/T/A)
-----  -----  -----  -----  -----  ---
-----  -----  -----  -----  -----  ---
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command	Description
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match probe-report

```
show ap arm client-match probe-report
  ap-name <name>
  ip-addr <ipaddr>
  ip6-addr <ip6-addr>
  assoc
  phy-type 802.11a|802.11b|80211g
```

Description

If ClientMatch is enabled, the output of this command displays the client probe report for the specified AP. APs using ClientMatch maintain a table of clients that have sent probe requests, and the signal-to-noise ratio (SNR) of the frame the AP received from the client. The AP sends these reports to the managed device every 30 seconds and the managed device forwards this information to the Mobility Conductor, which uses the information in these reports to steer each client to its optimal AP.

Parameter	Description
ap-name <name>	Name of the AP for which you want to view a client report.
ip-addr <ip-addr>	IPv4 address of an AP for which you want to view a client probe report.
ip6-addr <ip6-addr>	IPv6 address of an AP for which you want to view a client probe report.
assoc	Show information for associated clients only.
phy-type	Show information for one of the following phy types: <ul style="list-style-type: none">■ 802.11a■ 802.11b■ 80211g

Example

```
(host)#show ap arm client-match probe-report ap-name <ap-name>

AP Client Probe Report for Wifi0
-----
Client MAC          Signal  Assoc  Sec since   Sec since   Last heard
-----  -----  -----  -----  -----  -----
00:24:d7:40:ca:88  15      0      49          10          Wed Apr 10
01:20:46 2013
```

```

00:26:c6:4d:2b:74 21 0 23 10 Wed Apr 10
01:21:12 2013
00:1e:65:2b:7a:3e 23 0 55 10 Wed Apr 10
01:20:40 2013
74:e5:43:4b:3b:ff 34 0 20 10 Wed Apr 10
01:21:15 2013
AP Client Probe Report for Wifil
-----
Client MAC          Signal  Assoc  Sec since  Sec since  Last heard
      last heard    last reported
-----
22:33:44:55:66:77 50     0      6          9          Wed Apr 10
01:21:29 2013
c8:f7:33:29:82:db 41     0      60         9          Wed Apr 10
01:20:35 2013
ac:81:12:59:5c:12 32     0      50         9          Wed Apr 10
01:20:45 2013
00:24:d7:40:bb:b0 31     0      58         9          Wed Apr 10
01:20:37 2013
00:1a:73:15:8c:5f 32     0      57         9          Wed Apr 10
01:20:38 2013

```

The output of this command includes the following parameters:

Column	Description
Client MAC	AP name of the AP from which the client can detect a signal.
Signal	Signal strength, in dBm, of the probe request received from the client.
Assoc	A "Y" in this field indicates that the client is currently associated to that AP radio.
Sec since last heard	Time elapsed since the AP radio heard from the client.
Sec since last reported	Time elapsed since the AP radio heard from the client.
Last heard	Date and time at which the AP last heard from the client

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command	Description
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```
show ap arm client-match radio-summary
```

Description

If the Client Match feature is enabled, the output of this command displays the summary of radios in the network. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Example

```
(host) [mynode] #show ap arm client-match radio-summary
Radio Summary
-----
Radio BSSID          AP Name          Phy Type          Client-Pref  Num Clients
Num HE Clients
-----
-----
ac:a3:1e:88:b2:30    Usha_AP_205_26  5GHz (Non-HE)    Allow-All    0
0
ac:a3:1e:88:b2:20    Usha_AP_205_26  2.4GHz (Non-HE)  Allow-All    0
0
Num Active Radios:2
Num HE-Pref Radios:0
Num Non-HE-Pref Radios:0
Num Clients:0
Num HE Clients:0
```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.

Command	Description
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match rules

show ap arm client-match rules

Description

If the client match feature is enabled, the output of this command shows the rules of AP association changes triggered by the client match feature.

Examples

```
(host)[mm]#show ap arm client-match rules
ARM Client Match Rule Table
-----
ID  Env ID  Mac/Devtype  Steer Restrict  Steer Intvl  Override dot11v
Device cap  CM Params
--  --
-----
0   0       Ipad         None           300*         No           D
18/10/65/65/45/0/10/10000*/1*/1*/30/30/5/20/30/15/5/100/200/55/
1   0       Ipod         None           300*         No           None
18/10/65/65/45/0/10/10000*/1*/1*/30/30/5/20/30/15/5/100/200/55/
2   0       Iphone       None           300*         No           D
18/10/65/65/45/0/10/10000*/1*/1*/30/30/5/20/30/15/5/100/200/55/
3   0       Android      None           0            No           D
18/10/65/65/45/0/10/5/1*/1*/30/30/5/20/30/15/5/100/200/55/
* indicates non-default value
Steer Restrict Flags S: Sticky L: Load Balance H:HE Steer B: Bandsteer
Device Cap Flags D: Dual network
Override dot11v: Rule based 802.11v usage for steer
Params: Sticky low SNR/Sticky delta SNR/Sticky min signal
Bandst min A sig/Bandst max G sig
Abridged bit for 11v BTM/Steer restriction window
dot11v BTM attempts/Disassoc Imm/Pref Cand List
LB SNR Thr/LB Client Thr/LB Sig Delta/LB Thr Pct
MU SNR Thr/MU Client Thr/MU Sig Delta
dot11v Disassoc Timer/dot11v Validity Intvl/HE min sig
```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command	Description
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match restriction-table

```
show ap arm client-match restriction-table
  ap-name <name>
  ip-addr <ipaddr>
  ip6-addr <ip6-addr>
```

Description

If ClientMatch is enabled, the output of this command displays the list of clients that ClientMatch has restricted from the specified AP. These lists of restricted clients help the client associate to the best AP, by preventing the client from associating with a sub-optimal AP radio. The output of this command shows a list of all clients that were ever blacklisted from the specified AP.

Parameter	Description
ap-name <name>	Name of the AP for which you want to view the list of restricted clients
ip-addr <ipaddr>	IPv4 address of the AP for which you want to view the list of restricted clients
ip6-addr <ip6addr>	IPv6 address of the AP for which you want to view the list of restricted clients

Example

```
(host)[node] #show ap arm client-match restriction-table ap-name <ap-name>

Client Restriction Table for Wifi0
-----
Client MAC           Time last restricted   Restricted(Cur/Last)
-----
24:77:03:32:88:ec   Wed Apr 10 03:51:00 2014  0

PS deauth   Probe(home/scan/bc_ssid)   Auth(home/scan)
-----
-           2/0/no                     4/0

Time since last restriction(sec)   Radio Bssid
-----
18603                               00:1a:1e:89:c0:d0

Client Restriction Table for Wifi1
-----
Client MAC           Time last restricted   Restricted(Cur/Last)
-----
24:77:03:32:7b:cc   Wed Apr 10 03:47:16 2014  0
```

```

PS deauth   Probe(home/scan/bc_ssid)  Auth(home/scan)
-----
0/0/no     0/0/no                          0/0

Time since last restriction(sec)  Radio Bssid
-----
3866                             00:1a:1e:89:c0:c0

```

The output of this command includes the following parameters:

Column	Description
Client MAC	Displays the MAC address of the client that Client Match is attempting to steer.
Time last restricted	Displays the date and time at which the client was last steered in the vicinity of this radio.
Restricted(Cur/Last)	A "1" in this field indicates that the client is currently in the process of being steered to another radio.
PS deauth	Displays if the client is in power save mode when client match is attempting to steer the client.
Probe(home/scan/bc_ssid)	Displays the number of probe requests received on home channel, AP scanning, and SSID broadcast probe.
Auth(home/scan)	Displays the number of probe requests received on home channel and AP scanning for 802.11 authentication frames.
Time since last restricted	Display the time (in seconds) since the client was last steered in the vicinity of this radio.
Radio Bssid	Displays the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command	Description
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output will display Client Restriction Table for Wifi2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match summary

```
show ap arm client-match summary [client-mac <macaddr>] |[advanced] |[brief]
```

Description

If the client match feature is enabled, the output of this command shows the history of AP association changes triggered by the client match feature.

Parameter	Description
client-mac <macaddr>	MAC address of a client for which you want to view a history of AP association changes triggered by the client match feature.
advanced	Displays advanced debugging information. Include this parameter only under the supervision of Aruba support.
brief	Displays brief statistical information containing the final calculated data of the output parameters.

Example

The following command displays information on the Client Match summary. (For versions prior to ArubaOS 8.10.0.0.)

```
((host) [mynode](config) #show ap arm client-match summary

SM: Sticky Moves, BM: Bandsteer Moves, LM: Load Balance Moves, MU: MUsteer
Moves, VoM: Voice Roam M

oves, HM: HE Moves
T: Total, S: Success
ACC: Accept, REJ#: Reject with reason #, TO: Timeout FA: False Accept
11v Move Format: (T/ACC/REJ1/REJ2/REJ3/REJ4/REJ5/REJ6/REJ7/REJ8/TO/FA)
Client Match Summary
-----
MAC SM (T/S) LM (T/S) BM (T/S) MU (T/S) VoM (T/S) HM (T/S) Moves
(T/S) Last Move (Time/Rsn/

Dur)) Device Type 11v Moves
-----
-----

-----
Total clients:0
Sticky (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
Load-balance (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
Band-steer (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
```

```
Voice-roam (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
MU-Steer (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
HE-steer (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
```

The following command displays information on the Client Match summary. (For ArubaOS 8.10.0.0 or later versions.)

```
(host) [mynode] (config) #show ap arm client-match summary

SM: Sticky Moves, B5G: Bandsteer Moves to 5GHz, LM: Load Balance Moves, MU:
MUsteer Moves, VoM: Voice Roam Moves, HM: HE Moves, HP: HE Pooling Moves,
B6G: Bandsteer Moves to 6GHz
T: Total, S: Success
ACC: Accept, REJ#: Reject with reason #, TO: Timeout FA: False Accept
11v Move Format: (T/ACC/REJ1/REJ2/REJ3/REJ4/REJ5/REJ6/REJ7/REJ8/TO/FA)
Client Match Summary
-----
MAC                SM (T/S)  LM (T/S)  B5G (T/S)  MU (T/S)  VoM (T/S)  HM
(T/S)  HP (T/S)  B6G (T/S)  Moves (T/S)  Last Move (Time/Rsn/Dur))
      Device Type  11v Moves
-----
fc:b3:bc:43:f9:13  4/4      0/0      39/0      0/0      3/1      0/0
0/0      0/0      46/5      Oct 27 12:00:46 2021/Band-steer to
5GHz/X      39/1/0/0/0/0/0/0/2/0/23/13

Total clients:1
Sticky (T/S):4/4 Deauth (T/S):4/4 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
Load-balance (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
Band-steer to 5GHz (T/S):39/0 Deauth (T/S):0/0 11v-BTM:
39/1/0/0/0/0/0/0/2/0/23/13
Voice-roam (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
MU-Steer (T/S):3/1 Deauth (T/S):3/1 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
HE-steer (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
HE-pooling (T/S):0/0 Deauth (T/S):0/0 11v-BTM: 0/0/0/0/0/0/0/0/0/0/0
Band-steer to 6GHz (T/S):0/0 Deauth (T/S):0/0 11v-BTM:
0/0/0/0/0/0/0/0/0/0/0
```

The output of this command includes the following parameters.

Column	Description
MAC	MAC address of the client that was moved to a different AP radio.

Column	Description
<p>SM (T/S) Sticky Moves</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to move a mobile roaming client because it was staying associated (sticking) to a sub-optimal AP. ■ S: Number of times the client match successfully moved a mobile roaming client because it was staying associated (sticking) to a sub-optimal AP.
<p>LM (T/S) Load Balance Moves</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to move an AP to a different radio on dual-radio AP to balance the client load between the AP radios. ■ S: Number of times the client match feature successfully moved an AP to a different radio on dual-radio AP to balance the client load between the AP radios.
<p>BM (T/S) Bandsteer Moves (For versions prior to ArubaOS 8.10.0.0.)</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to steer

Column	Description
	<p>a dual-band client to a 5 GHz radio.</p> <ul style="list-style-type: none"> ■ S: Number of times the client match feature successfully moved a dual-band client to a 5 GHz radio.
<p>B5G (T/S) Bandsteer Moves to 5GHz (For ArubaOS 8.10.0.0 or later versions)</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to steer a dual-band client to a 5 GHz radio. ■ S: Number of times the client match feature successfully moved a dual-band client to a 5 GHz radio.
<p>B6G (T/S) Bandsteer Moves to 6GHz (For ArubaOS 8.10.0.0 or later versions)</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to steer a dual-band client to a 6 GHz radio. ■ S: Number of times the client match feature successfully moved a dual-band client to a 6 GHz radio.
<p>MU (T/S) MU steer Moves</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the Client Match feature attempted to steer and align MU-MIMO-capable clients with MU-

Column	Description
	<p>MIMO-capable radios.</p> <ul style="list-style-type: none"> ■ S: Number of times the client match feature successfully moved an AP to a different radio.
<p>VoM (T/S) Voice Roam Moves</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to move a voice client roaming from one AP BSS to another AP BSS using the same SSID. ■ S: Number of times the client match feature successfully moved a roaming voice client roaming from one AP BSS to another using AP BSS the same SSID.
<p>Moves (T/S)</p>	<p>The output of this column shows the following two values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to move an AP to a different radio. ■ S: Number of times the client match feature successfully moved an AP to a different radio.

Column	Description
Last Move	<p>This column shows the date and time the client was steered to a different AP radio, the reason why the client match feature made the change, and the number of seconds it took for the change to take place. Possible reasons include:</p> <ul style="list-style-type: none"> ■ Sticky: A mobile roaming client was staying associated (sticking) to a sub-optimal AP for too long. ■ Band steer: A dual-band capable client was steered toward a 5Ghz radio on a dual-band AP. ■ Band Balance: A dual-band capable client was steered toward a different radio to balance the load between the two radios on a single AP. ■ Load Balance: Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected from each underutilized AP. ■ ■ HE-Steer: A HE capable client was steered to a HE capable AP on the same band.

Column	Description
Device type	Type of client, if the value can be determined.
11v Moves (T/ACC/REJ1/REJ2/REJ3/REJ4/REJ5/REJ6/REJ7/REJ8/TO/FA)	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ■ T: Total number of times the client match feature attempted to move an AP to a different radio using the 802.11v BSS transition management request. ■ ACC: Number of times a client returned a 802.11v accept message. ■ REJ1: Move Rejected; unspecified reject reason ■ REJ2: Move Rejected; Insufficient Beacons ■ REJ3: Move Rejected; Insufficient capacity ■ REJ4: Move Rejected; BSS Termination undesired ■ REJ5: Move Rejected; BSS Termination Delay requested ■ REJ6: Move Rejected; STA BSS Trans List provided ■ REJ7: Move Rejected; No Suitable candidate ■ REJ8: Move Rejected; Leaving ESS ■ TO: Number of times the dot11v

Column	Description
	<p>BSS transition management request timed out because the client failed to acknowledge the 802.11v BSS transition management request from the AP.</p> <ul style="list-style-type: none"> ■ FA: Number of false accepts, where the client responds to a move request with an accept message, but fails to move to the destination radio and remains on the same radio.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match restriction-table	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Command	Modification
ArubaOS 8.10.0.0	The output of the <code>show ap arm client-match summary</code> and <code>show ap arm client-match summary advanced</code> commands was modified to include the following fields for Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ B5G (T/S) ■ B6G (T/S)
ArubaOS 8.6.0.0	The output of the <code>show ap arm client-match summary advanced</code> command was modified to display the percentage of ClientMatch success in addition to the absolute values.
ArubaOS 8.3.0.0	A new parameter <code>brief</code> was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm client-match unsupported

show ap arm client-match unsupported

Description

If the client match feature is enabled, the output of this command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered. The controller also keeps track of the number of times the client match feature failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If the client match feature attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as un-steerable for that specific trigger.

Example

The following example displays a list of unsteerable clients. (For versions prior to ArubaOS 8.10.0.0.)

```
(host) [mynode] (config) #show ap arm client-match unsupported

Client Match Unsteerable Clients
-----
MAC  Unsteerable Flags  Last Steer Time  Expiry Time  Total
steers/successful
---  -----
-
S: Sticky L: Load Balance H: HE Steer B: Bandsteer I: IOS T: Temporary D(I):
dot 11v IOS M: MU steer (R): Rule based Vo: Voice Roam
Total Unsteerable Clients:0
=====
=====
```

The following example displays a list of unsteerable clients. (For ArubaOS 8.10.0.0 or later versions.)

```
(host) [mynode] (config) #show ap arm client-match unsupported

Client Match Unsteerable Clients
-----
MAC  Unsteerable Flags  Last Steer Time  Expiry Time  Total
steers/successful
---  -----
-
S: Sticky L: Load Balance H: HE Steer B5G: Bandsteer to 5GHz B6G: Bandsteer
to 6GHz I: IOS T: Temporary D(I): dot11v IOS Mr: MU steer (R): Rule based
Vo: Voice Roam P: HE-Pooling
```



```
Total Unsteerable Clients:0
```

The output of this command includes the following parameters:

Column	Description
MAC	MAC address of the client that could not be steered to a different AP radio.
Unsteerable Flags	<p>The client is marked unsteerable under specific client steer triggers. These triggers include:</p> <ul style="list-style-type: none">■ Sticky: A mobile roaming client is staying associated (sticking) to a sub-optimal AP for too long.■ Bandsteer: A dual-band capable client is steered towards a 5 GHz radio on a dual-band AP. (For versions prior to ArubaOS 8.10.0.0.)■ Bandsteer to 5GHz: A dual-band capable client is steered towards a 5 GHz radio on a dual-band Wi-Fi 6E AP. (For ArubaOS 8.10.0.0 or later versions.)■ Bandsteer to 6GHz: A dual-band capable client is steered towards a 6 GHz radio on a dual-band Wi-Fi 6E AP. (For ArubaOS 8.10.0.0 or later versions.)■ Load Balance: Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected from each underutilized AP.■ IOS: An IOS device is temporarily prevented from steering to avoid blacklisting/denylisting the ESS.■ Temporary: A client is temporarily prevented from steering after undergoing a successful band steer, then reverting back to a 2.4GHz radio.■ HE Steer: HE Steer will not be attempted for the client.■ MU Steer: MU Steer will not be attempted for the client■ Dot 11v IOS: IOS client has been marked unsteerable for steers.■ Rule based: Client has been marked unsteerable by Rules Based Client Match (RBCM).■ Voice Roam: Voice roam steer will not be attempted for the client.
Last Steer Time	Timestamp showing the date and time the client match feature failed to associate the client to a different AP radio.
Expiry Time	The amount of time before a client steer attempt expires.
Total steers/successful	The total number of client steer attempts, and the number of successful client steer attempts.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match restriction-table	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Command	Modification
ArubaOS 8.10.0.0	The command output was modified to include the following flags for Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ B5G ■ B6G
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm history

```
show ap arm history {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

For each interface on an AP, this command shows the history of the channel and power changes due to Adaptive Radio Management (ARM).

Parameter	Description
ap-name <ap-name>	Show ARM history for an AP with a specific name.
bssid <bssid>	Show ARM history for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show ARM history for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Example

Adaptive Radio Management (ARM) can automatically change channel and power levels based on a number of factors such as noise levels and radio interference.

The following example shows an AP's channel and power changes over time, and the reason why those changes took place (For versions prior to ArubaOS 8.9.0.0).

```
(host)[node]#show ap arm history ap-name AP-16
Interface :wifi0
ARM History
-----
Reason  Old channel  New channel  Old Power  New Power  Last change
-----  -
P-      153-         153-        12         9         3d:14h:56m:48s
P+      153-         153-        9          12        3d:13h:44m:7s
P+      153-         153-        12         15        3d:13h:23m:5s
P+      153-         153-        15         18        3d:13h:16m:32s
P+      153-         153-        18         21        3d:11h:42m:42s
P-      153-         153-        21         15        3d:8h:16m:12s

Interface :wifi1
ARM History
-----
Reason  Old channel  New channel  Old Power  New Power  Last change
-----  -
P-      11          11          15         12        3d:18h:22m:28s
P+      11          11          12         15        3d:18h:17m:27s
P-      11          11          15         12        3d:18h:9m:9s
P+      11          11          12         15        3d:17h:48m:41s
```

```

P+      11      11      15      18      3d:17h:44m:34s
P-      11      11      18      15      3d:17h:39m:11s
P-      11      11      15      12      3d:17h:32m:39s
P+      11      11      12      15      3d:17h:26m:15s
I: Interference, R: Radar detection, N: Noise exceeded, E: Error threshold
exceeded, INV: Invalid Channel, G: Rogue AP Containment, M: Empty Channel,
P+: Increase Power, P-: Decrease Power, OFF: Turn off Radio, ON: Turn on
Radio

```

The following example shows an AP's channel and radio band (ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap arm history ap-name hhm-635

Interface :wifi0
Phy-Type  :5GHz
Interface :wifi1
Phy-Type  :2.4GHz
Interface :wifi2
Phy-Type  :6GHz
I: Interference, R: Radar detection, N: Noise exceeded, Q: Bad Channel
Quality E: Error threshold exceeded, INV: Invalid Channel, G: Rogue AP
Containment,
M: Empty Channel, P+: Increase Power, P-: Decrease Power, 40INT: 40MHZ
intol detected on 2.4G, NO40INT: 40MHZ intol cleared on 2.4G,
OFF(R): Turn off Radio due to Radar, OFF(MA): Turn off Radio due to Mode
Aware, ON: Turn on Radio, D: Dynamic Bandwidth Switch, AIRMATCH: AirMatch
Event,
I*: CCA Interference, C: Radar cleared, NC: Noise Cleared, Random: Random
Channel, RMC: Radio Mode Change, RCP: Radio Client Preference Change,
OFF(C) : Turn off Radio due to config

```

The output of this command includes the following information:

Column	Description
Phy-Type (ArubaOS 8.9.0.0 or later versions)	The PHY type of the radio. Possible values are 2.4GHz , 5GHz , or 6GHz .
Reason	This column displays one of the following code to indicate why the channel or power change was made. <ul style="list-style-type: none"> ■ I: Interference ■ R: Radar detected ■ N: Noise exceeded ■ E: Error threshold exceeded ■ INV: Invalid Channel ■ G: Rogue AP Containment ■ M: Empty Channel ■ P+: Increase Power ■ P-: Decrease Power ■ OFF: Turn off Radio ■ ON: Turn on Radio

Column	Description
	The Reason key appears at the bottom of the ARM History table.
Old Channel	Channel number used by the AP interface before the ARM change.
New Channel	Channel number used by the AP interface after the ARM change.
Old Power	Power level of the AP interface before the ARM change.
New Power	Power level of the AP interface after the ARM change.
Last Change	Time elapsed since the change, in the format <i>days:hours:minutes:seconds</i> .

Related Commands

Command	Description
<u>rf arm-profile</u>	This command enables ClientMatch.
<u>show ap arm client-match probe-report</u>	This command displays the client probe report for the specified AP.
<u>show ap arm client-match neighbors</u>	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>Phy-Type</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm neighbors

```
show ap arm neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the ARM settings for an AP's neighbors.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The following example shows ARM neighbor information for AP name **ap70_1**(For versions prior to ArubaOS 8.9.0.0).

```
(host)[node]# show ap arm neighbors ap-name ap70_1

BSSID: BSSID of discovered radio
ESSID: ESSID of discovered radio/Src BSSID through which the neighbor is
discovered
Channel: Channel of operation of discovered radio
SNR: Signal to noise ratio of discovered radio
tx-power: Tx Power of discovered radio (if known)
PL: Path loss to discovered radio (using txpower and SNR)
AP Flags: Active: Discovered using OTA updates
          Passive: Discovered using passive scan
          Indirect: Two hop neighbors discovered using neighbors OTA update
Last Update: Timestamp when last OTA update was received (total OTA updates)

ARM Neighbors
-----
BSSID          ESSID          Channel  SNR  Tx-power  PL (dB)  AP Flags
Last Update (Total updates)
-----
-----
6c:f3:7f:b6:68:14  ssid-ap1      153      49   22        69      Passive
18:64:72:93:6a:f2  ssid-ap2      132      48   24        68      Passive
18:64:72:02:24:30  ssid-ap3      153      47   18        63      Passive
18:64:72:01:f8:f0  ssid-ap4      36       60   22         0      Indirect
2015-03-12 16:38:26
9c:1c:12:fe:96:e4  ssid-ap5      11       33   18       123     Indirect
```

```

2015-03-13 08:37:18
6c:f3:7f:4b:64:23 ssid-ap6 6 51 20 125 Active
2015-03-12 14:05:48

```

The following example shows ARM neighbor information for Wi-Fi 6E AP name **hhm-635**(For ArubaOS 8.9.0.0 or later versions).

```

(Aruba7210-standalone-hhm) ^*[mynode] (config) #show ap arm neighbors ap-
name hhm-635

BSSID: BSSID of discovered radio
ESSID: ESSID of discovered radio/Src BSSID through which the neighbor is
discovered
Channel: Channel of operation of discovered radio
SNR: Signal to noise ratio of discovered radio
tx-power: Tx Power of discovered radio (if known)
PL: Path loss to discovered radio (using txpower and SNR)
AP Flags: Active: Discovered using OTA updates
          Passive: Discovered using passive scan
          Indirect: Two hop neighbors discovered using neighbors OTA update
Last Update: Timestamp when last OTA update was received (total OTA updates)

ARM Neighbors
-----
bssid          essid          phy-type  channel  snr  tx-power
PL (dB)  AP Flags  Last Update (Total updates)
-----  -
-----  -
1c:28:af:68:66:40  11            6GHz     37+     34  16
72      Passive
1c:28:af:68:66:41  060606        6GHz     37+     33  16
72      Passive
1c:28:af:68:55:c0  ethersphere-arubaos-6g  6GHz     201E    7   9
92      Active    2021-07-22 14:46:37 (21342)
1c:28:af:68:28:c0  jiyong-remote  6GHz     145E    16  20
95      Passive
cc:88:c7:41:25:30  ethersphere-arubaos-6g  6GHz     53E     4   9
96      Active    2021-07-22 13:09:47 (181)
20:4c:03:80:00:20  aruba-ap      6GHz     37E     17  21
94      Active    2021-07-22 14:46:42 (10108)
1c:28:af:68:11:20  liying-635    6GHz     37S     33  21
78      Passive
1c:28:af:68:17:b2  000jiajuntest111  6GHz     37S     4   15
101     Active    2021-07-22 14:14:00 (5)

```

The output of this command includes the following information:

Column	Description
BSSID	BSSID of the discovered radio of the AP.

Column	Description
ESSID	ESSID of the discovered radio of the AP or source BSSID through which the neighbor is discovered.
Channel	Channel of operation of the discovered radio of the AP.
phy-type (ArubaOS 8.9.0.0 or later versions)	Radio band of the AP. Displays one of the following values: <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz (For Wi-Fi 6E APs)
SNR	Signal to noise ratio of the discovered radio of the AP.
Tx-power	Transmitter power of the discovered radio of the AP (if known).
PL (db)	Path loss to the discovered radio (using tx-power and SNR)
AP Flags	<ul style="list-style-type: none"> ■ Active: Discovered using Over-The-Air (OTA) updates ■ Passive: Discovered using passive scan ■ Indirect: Two hop neighbors discovered using neighbors OTA update
Last Update	Time stamp when last OTA update was received (total OTA updates)

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes:(ArubaOS 8.9.0.0 or later versions) <ul style="list-style-type: none"> ■ Added <code>phy-type</code> parameter. ■ Added 2.4GHz, 5GHz, and 6GHz values for <code>phy-type</code>

Release	Modification
	parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm rf-summary

```
show ap arm rf-summary {ap-name <ap-name>|{bssid <bssid>|{ip-addr <ip-addr>}  
[verbose]
```

Description

Show the state and statistics for all channels being monitored by an individual AP.

Parameter	Description
ap-name <ap-name>	Show channel data for an AP with a specific name.
bssid <bssid>	Show channel data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show channel data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.
verbose	(Optional) Include the channel quality history for all channels on the AP's radios in the output of this command.

Examples

The following example shows detailed information for the individual channels being monitored and statistics for each AP interface (For versions prior to ArubaOS 8.9.0.0). Use this command to verify an AP's RF health, or to determine why multiple APs in the same area are on the same channel.

```
(host)[node] #show ap arm rf-summary ap-name AP-205  
Channel Summary  
-----  
channel  retry  phy-err  mac-err  noise  util(Qual)  cov-idx(Total)  intf_  
idx(Total)  
-----  
-----  
36      0      0      0      92      0/0/0/0/95  0/0(0)  
118/18//0/0(136)  
40      0      0      0      89      8/1/2/1/95  0/0(0)  
139/47//0/0(186)  
44      0      0      0      89      7/0/2/2/95  0/0(0)  
117/36//0/0(153)  
48      0      0      0      89      10/3/2/0/96 0/0(0)  
175/109//0/0(284)  
52      0      0      0      90      9/2/2/2/95  0/0(0)  
328/87//0/0(415)  
56      0      0      0      90      6/0/2/3/96  0/0(0)  
81/128//0/0(209)
```

```

60      0      0      0      89      8/1/2/0/95      0/0(0)
385/49//0/0(434)
64      0      0      0      90      8/1/2/1/95      0/0(0)
65/0//0/0(65)
149     0      0      0      92      7/3/0/0/94      0/0(0)
349/48//0/0(397)
153     0      0      0      93      6/6/0/0/95      0/0(0)
428/105//0/0(533)
157     0      0      0      92      10/3/2/0/95     0/0(0)
290/229//0/0(519)
161     0      0      9      92      4/1/0/6/95      7/0(7)
308/114//0/0(422)
11      0      0      10     91      58/51/1/0/94    7/0(7)
1064/284//0/0(1348)

```

Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality

HT Channel Summary

```

-----
channel_pair  Pairwise_intf_index
-----

```

```

149-153      930
157-161      941

```

```

Interface Name      :wifi0
Current ARM Assignment :161-/21
Covered channels a/g :1/0
Free channels a/g    :3/0
ARM Edge State      :disable
Last check channel/pwr :7m:13s/22s
Last change channel/pwr :32m:22s/10h:15m:40s
Next Check channel/pwr :33s/4m:43s
Assignment Mode      :Single Band
Interface Name      :wifil
Current ARM Assignment :11/21
Covered channels a/g :0/1
Free channels a/g    :0/0
ARM Edge State      :disable
Last check channel/pwr :3m:25s/2m:1s
Last change channel/pwr :10h:15m:40s/10h:15m:40s
Next Check channel/pwr :1m:4s/3m:59s
Assignment Mode      :Single Band

```

The following is the output for AP-555 access points,
(host) [mynode] #show ap arm rf-summary ap-name AP555

Channel Summary

```

-----
channel band      retry  phy-err  mac-err  noise  util(Qual)  cov-idx(Total)
intf_idx(Total)
-----
-----
36      2.4GHz      0      0      0      92      1/1/0/0/100  0/0(0)
29/0//0/0(29)
40      5GHz      0      0      0      92      23/17/0/0/94  0/0(0)
14/10//0/0(24)
44      6GHz      0      0      0      92      0/0/0/0/100  0/0(0)
6/0//0/0(6)

```

Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality

Noise followed by "*" indicates that the last scan on this channel was a split-scan, which was triggered by high channel noise. Check show ap arm split-scan-history.

HT/VHT Channel Summary

Bandwidth	Channel range	Total interference index
40MHz	36-40	53
40MHz	44-48	16
40MHz	149-153	131
40MHz	157-161	85
80MHz	149-161	216

```

Interface Name           :wifi0
Current ARM Assignment   :153E/0.0/5GHz
Covered channels a/g    :4/0
Free channels a/g       :0/0
Last check channel/pwr  :10h:35m:51s/10h:35m:51s
Last change channel/pwr :10h:35m:51s/10h:35m:51s
Next Check channel/pwr  :0s/0s
Assignment Mode         :Disable
Interface Name           :wifi1
Current ARM Assignment   :9+/0.0
Covered channels a/g    :0/3
Free channels a/g       :0/0
Last check channel/pwr  :10h:35m:51s/10h:35m:51s
Last change channel/pwr :10h:35m:51s/10h:35m:51s
Next Check channel/pwr  :0s/0s
Assignment Mode         :Disable
Interface Name           :wifi2
Current ARM Assignment   :157E/15.2
Covered channels a/g    :8/0
Free channels a/g       :0/0
ARM Edge State          :disable
Last check channel/pwr  :10h:35m:51s/10h:35m:51s
Last change channel/pwr :10h:35m:51s/10h:35m:51s
Next Check channel/pwr  :0s/0s
Assignment Mode         :Disable

```

The following example shows detailed information for the individual channels being monitored and statistics for each AP interface (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #show ap arm rf-summary ap-name hhm-635
```

Channel Summary

phy-type	channel	retry	phy-err	mac-err	noise	util(Qual)	cov-idx
(Total)	intf_idx(Total)						
6GHz	21	0	0	0	90	0/0/0/0/100	0/0(0)
	0/0//0/0(0)						
6GHz	25	0	0	0	92	0/0/0/0/100	0/0(0)

0/0//0/0(0)							
6GHz 29	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 33	0	0	0	92	0/0/0/0/100	0/0(0)	
0/6//0/0(6)							
6GHz 125	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 129	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 133	0	0	0	92	0/0/0/0/100	0/0(0)	
1/0//0/0(1)							
6GHz 137	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 141	0	0	0	92	0/0/0/0/100	0/0(0)	
0/1//0/0(1)							
6GHz 145	0	0	0	91	0/0/0/0/100	0/0(0)	
3/0//0/0(3)							
6GHz 149	0	0	0	91	0/0/0/0/100	0/0(0)	
0/1//0/0(1)							
6GHz 153	0	0	0	91	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 157	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 161	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 165	0	0	0	91	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 169	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 173	0	0	0	91	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 177	0	0	0	95	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 181	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 185	0	0	0	95	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 189	0	0	0	91	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 193	0	0	0	92	0/0/0/0/100	0/0(0)	
1/0//0/0(1)							
6GHz 197	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 201	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 205	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 209	0	0	0	95	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 213	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 217	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 221	0	0	0	92	0/0/0/0/100	0/0(0)	
0/0//0/0(0)							
6GHz 225	0	0	0	95	0/0/0/0/100	0/0(0)	

```

0/0//0/0(0)
6GHz      229      0      0      0      95      0/0/0/0/100  0/0(0)
0/0//0/0(0)
6GHz      233      0      0      0      95      0/0/0/0/100  0/0(0)
0/0//0/0(0)

```

Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality
 Noise followed by "*" indicates that the last scan on this channel was a split-scan, which was triggered by high channel noise. Check show ap arm split-scan-history.

HT/VHT Channel Summary

```

-----
Phy-Type  Bandwidth  Channel range  Total interference index
-----
6GHz      80MHz      97-109         0
6GHz      80MHz      145-157        4
6GHz      80MHz      193-205        1
6GHz      80MHz      33-45          31
6GHz      80MHz      81-93          0
6GHz      80MHz      129-141        2
6GHz      80MHz      177-189        0
6GHz      80MHz      65-77          0
6GHz      80MHz      113-125        0
6GHz      80MHz      161-173        0
6GHz      80MHz      209-221        0
6GHz      80MHz      49-61          12

```

```

Interface Name      :wifi2
Phy-Type            :6GHz
Current ARM Assignment :37S/15.0
Covered channels 5/2.4/6GHz :7/0/32
Free channels 5/2.4/6GHz :0/0/0
ARM Edge State      :disable
Last check channel/pwr :20d:18h:18m:21s/20d:18h:18m:21s
Last change channel/pwr :20d:18h:18m:21s/20d:18h:18m:21s
Next Check channel/pwr :0s/0s
Assignment Mode      :Disable

```

The output of this command includes the following information:

Column	Description
phy-type (ArubaOS 8.9.0.0 or later versions)	The PHY type of the radio. Possible values are 2.4GHz , 5GHz , or 6GHz .
channel	Number of a radio channel used by the AP.
band	Displays the band, 2.4 GHz, 5 GHz, or 6 GHz.
retry	Number of 802.11 retry frames sent because a client failed to send an ACK.

Column	Description
phy-err	Number of PHY errors on the AP's current channel seen during the last second.
mac-err	Number of MAC errors on the AP's current channel seen during the last second.
noise	Current noise level, in -dBm.
util (Qual)	The quality of the channel based on the channel utilization.
cov-idx	The AP uses this metric to measure RF coverage. The coverage index is calculated as $x+y$, where "x" is the AP's weighted calculation of the Signal-to-Noise Ratio (SNR) on all valid APs on a specified 802.11 channel, and "y" is the weighted calculation of the Aruba APs SNR the neighboring APs see on that channel.
intf_idx	The AP uses this metric to measure co-channel and adjacent channel interference. The Interference Index is calculated as $a/b//c/d$, where: <ul style="list-style-type: none"> ■ Metric value "a" is the channel interference the AP sees on its selected channel. ■ Metric value "b" is the interference the AP sees on the adjacent channel. ■ Metric value "c" is the channel interference the AP's neighbors see on the selected channel. ■ Metric value "d" is the interference the AP's neighbors see on the adjacent channel. ■ To calculate the total Interference Index for a channel add "a+b+c+d".
Interface Name	Name of the gigabit Ethernet interface
Phy-Type (ArubaOS 8.9.0.0 or later versions)	The PHY type of the radio. Possible values are 2.4GHz , 5GHz , or 6GHz .
Current ARM Assignment	Current channels assigned by the AP's ARM profile.
Target Coverage Index	Ideal value of coverage index an AP tries to achieve on its channel.
Covered channels a/g	Number of channels that are currently being used by an AP's BSSIDs.
Free channels a/g	Number of channels that are available to an AP because that channel has a lower interference index.
ARM Edge State	If enabled, ARM-enabled APs on the network edge will not become Air Monitors.

Column	Description
<code>Last check channel/pwr</code>	Time elapsed since the AP checked its channel and power settings, in <i>hour:minute:second</i> format.
<code>Last change channel/pwr</code>	Time elapsed since the AP changed its channel and power settings, in <i>hour:minute:second</i> format.

Related Commands

Command	Description
<code>rf arm-profile</code>	This command enables ClientMatch.
<code>show ap arm client-match probe-report</code>	This command displays the client probe report for the specified AP.
<code>show ap arm client-match neighbors</code>	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
<code>show ap arm virtual-beacon-report</code>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<code>show ap arm client-match unsupported</code>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<code>show ap arm client-match summary</code>	This command shows the history of AP association changes triggered by the client match feature.
<code>show ap arm client-match history</code>	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>band</code> and <code>phy-type</code> parameters were introduced. The <code>band</code> is added at the end of the <code>Current ARM assignment</code> parameter.
ArubaOS 8.6.0.0	The output will display an interface report for Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm scan-times

```
show ap arm scan-times {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Shows channel scan times for an individual AP and information on the channel being scanned.

Parameter	Description
ap-name <ap-name>	Show channel scan data for an AP with a specific name.
bssid <bssid>	Show channel scan data for a specific Basic Service Set Identifier (BSSID) on an AP.
ip-addr <ip-addr>	Show channel scan data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows scan times for every channel on AP-225. All UTB blocked channels are marked with the flag u in the scan channel table.

```
(host)[node]#show ap arm scan-times ap-name AP-225

Channel Scan Time
-----
channel band      assign-time(ms)  scans-attempted  scans-rejected  scans-
deferred dos-scans flags            timer-tick
-----
---  -----  -----  -----
1    2.4GHz    796070          7237            0              0
   0          DACLYS          183703
36   5GHz      488400          4440            0              0
0    DA          183713
1    6GHz      231122          4440            0              0
   DA          183713

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity
Present
L: Scan Secondary Above, U: Scan Secondary Below, Y: Scan 80MHz, Z: Rare
Channel
V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel, P: Valid 40MHZ
Channel Pair
E: Valid 80MHz Channel (lower 20M), B: Belongs to valid 80MHz channel
O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N: Split Channel
Scan
R: Radar detected in last 30 min, X: DFS required, S: Transmit Allowed
J: Unconventional Scan 40MHz Above, M: Unconventional Scan 40MHz Below
e: Scan Preferred Channel
```

```

WIFI Channel Scanning State
-----
Scan mode      scan type      band/ch      band/current-scan-channel      last-dos-channel
timer-milli-tick
-----
Aggressive     DEF           2.4GHz/11    2.4GHz/11                      0

next-scan-milli-tick (jitter)  scans (Tot:Rej:Eff(%):Last intvl(%))
-----
0 (0)                1257:0:100:0

Group Scan Time
-----
channels      band      assign-time(ms)  scans-attempted  scans-rejected  scans-
deferred  group-width  timer-tick
-----
34          5GHz      113960           1036              0                0
          20MHz      183544
36,40,44,48  5GHz      3184390          28949             0                0
          80MHz      183711
38          5GHz      114070           1037              0                0
          20MHz      183575
42          6GHZ      114070           1037              0                0
          20MHz      183591
Zero Wait DFS Scan
-----
Scan mode Channel
-----
Look-ahead 100E

```

The output of this command displays UTB-filter-block for 6 GHz band.

```

(host)[mynode] (config) #show ap arm scan-times ap-name hhm-635

Channel Scan Time
-----
channel  band  assign-time(ms)  scans-attempted  scans-rejected  scans-
deferred  dos-scans  flags  timer-tick
-----
34      5GHz  0                0                0                0
        0      DYp            0
36      5GHz  0                0                0                0
        0      DVCLYETSp     0
1       6GHz  325270          2957             0                0
        0      DCLYWpu       953147
5       6GHz  493460          4486             2                0
        0      DCUYWJpxu     953214
9       6GHz  291610          2651             0                0
        0      DCLYWpu       953271

```

```

233      6GHz      4294468996      62028      62028      0
      0      DVCYWTP      0
Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity
Present, Y: Scan 80MHz,
      L: Scan Secondary Above, U: Scan Secondary Below, Z: Rare
Channel
      V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel, P:
Valid 40MHZ Channel Pair
      E: Valid 80/80+80MHz Channel (First 20M), B: Belongs to valid
80/80+80MHz channel
      G: Valid 160MHz Channel (First 20M), Q: Belongs to valid
160MHz channel
      O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N:
Split Channel Scan
      R: Radar detected in last 30 min, X: DFS required, S:
Transmit Allowed
      J: Unconventional Scan 40MHz Above, M: Unconventional Scan
40MHz Below
      b: Out-of-band scan Channel (valid only for dual 5GHz mode),
p: Pooling Preference
      q: Zero Wait DFS u: UTB filtered channel, W: Scan 160MHz,
t: Zero Wait DFS Test Mode, x: Preferred Scan Channel (6GHz
Only),
      e: Scan Preferred Channel

```

WIF Channel Scanning State

```

-----
Scan mode  channel  band  current-scan-channel  last-dos-channel  timer-
milli-tick  next-scan-milli-tick (jitter)
-----
-----
Default    0        5GHz   0                    0
945674170  0 (0)
Default    0        2.4GHz 0                    0
945674170  0 (0)
Aggressive 37S      6GHz   197E                 0
945674170  945675120 (-41)

```

```

scans (Tot:Rej:Eff(%):Last intvl(%))
-----
scans (Tot:Rej:Eff(%):Last intvl(%))
scans (Tot:Rej:Eff(%):Last intvl(%))
scans (Tot:Rej:Eff(%):Last intvl(%))

```

Group Scan Time

```

-----
channels  band  assign-time(ms)  scans-attempted  scans-rejected  scans-
deferred  group-width  timer-tick
-----
-----
1-29      6GHz  325270           2957              0                0
      160MHz  953147
1-29      6GHz  818730           7443              2                0
      160MHz  953214

```

UTB filter Info:

```

-----
Type   Version A1  Version A2  Version A3  Version A4  Channel Spacing
-----
LTCC   1             1           1           1           210 MHz

UTB filter results:
-----
Band selected  Last blocked channel
-----
6GHz          19

```

The output of this command includes the following parameters:

Column	Description
channel	Displays the channels in the group.
band	Displays the band, 2.4 GHz, 5 GHz, or 6 GHz.
assign-time (ms)	The cumulative time spent on the channel.
scans-attempted	The number of times an AP attempted to scan a channel.
scans-rejected	The number of times an AP attempted to scan a channel, but was unable to scan because the scan was halted by the power save, VoIP aware, video aware or load aware ARM features.
scans-deferred	The number of times an AP deferred to scan a channel due to an event such as a radar detection.
dos-scans	The number of times an AP visited the channel to contain a rogue device.
flags	Displays additional information about the channel. The flags key is displayed at the bottom of the Channel Scan Time table.
group_width	The channel width of the group.
timer-tick	The timer-tick of the last scan.
UTB filter results	
Band selected	Displays the band selected in the regulatory-profile, used by the AP that is queried. If the band selected is 5 GHz, the First blocked channel is displayed. If the band selected is 6 GHz, the Last blocked channel is selected.
First blocked channel	Displays the first channel blocked in the 5 GHz band. All the channels from this channel to the last channel of the 5 GHz band will be blocked.

Column	Description
Last blocked channel	Displays the last channel that is blocked in the 6 GHz band. All the channels from the start of the 6 GHz band until this channel will be blocked.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match probe-report	This command displays the client probe report for the specified AP.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.
show ap arm virtual-beacon-report	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
show ap arm client-match unsupported	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	<p>The command output was modified to include following parameters:</p> <ul style="list-style-type: none"> band <p>The command output was modified to include the UTB filter results, and based on the band selected the following parameters were displayed:</p> <ul style="list-style-type: none"> First blocked channel Last blocked channel <p>The help text e: Scan Preferred Channel is introduced.</p>
ArubaOS 8.8.0.0	The output was modified to include zero wait DFS channel details.

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm split-scan-history

```
show ap arm split-scan-history {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show scanning information for a "split-scan", where ARM performs an additional scans on each channel within a 40 MHz channel pair or 80 MHz channel set.

If ARM reports a high noise floor on a channel within a 40 MHz channel pair or 80 MHz channel set, ARM performs an additional 20 MHz scan on each channel within that channel pair or set, to determine the actual noise floor of each affected channel. This allows ARM to avoid assigning the overutilized channel, while still allowing channel assignments to the other unaffected channels in that channel pair or set.

Parameter	Description
ap-name <ap-name>	Show scan data for an AP with a specific name.
bssid <bssid>	Show scan data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show scan data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows information about one split-scan performed on channel 161E.

```
(host)[node]# show ap arm split-scan-history ap-name 1242-ac
Interface :wifi0
Split Scan History
-----
Time of setup           Channel scan   Number of Split scans   Noise Floor
-----
2013-10-08 03:11:40   161E          4                        69
Interface :wifi1
```

The output of this command includes the following parameters:

Column	Description
Time of setup	Timestamp showing the date and time the scan was performed

Column	Description
Channel Scan	The channel pair or channel set scanned
Number of Split Scans	The number of times ARM performed an additional split scan.
Noise Floor	Noise floor recorded on the primary channel within that channel pair or channel set.

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output will display an interface for Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm state

```
show ap arm state [ap-name <ap-name>|dot11a|dot11g|ip-addr <ip-addr>]
```

Description

Displays Adaptive Radio Management (ARM) information for an individual AP's neighbors, or show all available data for any neighboring AP using an 802.11a or 802.11g radio type. Include an AP name or IP address to show data for just a single AP, or use the **dot11a** or **dot11g** keywords to show data for all APs using that radio type.

Parameter	Description
ap-name <ap-name>	Show aggregate ARM Neighbor Information for a specific AP.
dot11a	Show aggregate ARM Neighbor Information for all APs using an 802.11a radio.
dot11g	Show aggregate ARM Neighbor Information for all APs using an 802.11g radio.
ip-addr <ip-addr>	Show aggregate ARM Neighbor Information for a AP with a specific IP address by entering its IP address in dotted-decimal format.

Examples

The output of this command shows 802.11a information for all neighboring APs.

```
(host)[node]# show ap arm state

show ap arm state ap-name AP49
AP-1249:10.100.139.233:52:21:26-Edge:disable : Client Density:13
Neighbor Data
-----
Name                IP Address SNR  Assignment  Neighbor Density
-----
AP42                10.100.139.249  41   52/21      13/17/100/76
AP09                10.100.139.224  22   56/21      3/5/23/60
AP48                10.100.139.241  36   60/21      9/11/69/81
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.

Column	Description
IP address	IP address of an AP.
SNR	Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Path loss	Path loss to the discovered radio (using tx-power and SNR)
Channel/Pwr	The AP's current channel assignment.
Neighbor Density	The neighborhood density for the specified AP is listed with the values A/B/C/D, where: <ul style="list-style-type: none"> ■ A= Number of the AP's clients heard in the AP neighbor's client list ■ B= Number of clients in AP neighbor's client list ■ C= Density percentage, (AP clients heard in in the AP neighbor client list / AP client density * 100). ■ D= Density Percentage (AP clients heard in the AP neighbor's client list / neighbor client density * 100)

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap arm status

```
show ap arm status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Run this command under the supervision of Aruba support to display detailed debugging Adaptive Radio Management (ARM) information and ARM status counters for an individual AP.

Parameter	Description
ap-name <ap-name>	Show ARM status for an AP with a specific name.
bssid <bssid>	Show ARM status for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show ARM status for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Example

The output of this command shows detailed debugging Adaptive Radio Management (ARM) information and ARM status counters for an individual AP:

```
(host) #show ap arm status ap-name AP_205
Interface:wifi0
ARM Internal State
-----
Variable                               State
-----
Radar detected                          FALSE
Invalid channel detected                 FALSE
Error detected                           FALSE
Noise detected                           FALSE
Channel quality detected                 FALSE
40MHz assignment                         TRUE
80MHz assignment                         TRUE
160MHz assignment                        FALSE
80+80MHz assignment                      FALSE
Secondary present                        TRUE
Multi-band assignment                    FALSE
Using default channel                     FALSE
Dynamic bw signatures detected           FALSE
ARM Status Counters
-----
Status                                   Count
-----
SAP Monitor No Mode Aware                0
```

```

Null current channel          0
40MHz Intol Detected         0
Hang Detected                 0
Hang Cleared                  0
ARM Disable/Maintain         0
ARM in Backoff                0
Client Aware                  0
ARM Clean Channel             0
ARM Min Scans                 0
ARM No Min Intf Channel       0
ARM 40M No Min Intf Channel   0
ARM 80M No Min Intf Channel   0
ARM 160M No Min Intf Channel  0
ARM Active rogue on home channel 0
ARM Delay Channel Change      0
ARM Channel Checks            17
ARM Channel Change            17
ARM Same 80MHz Channel         0
ARM Auto Bandwidth Mode Detected 0
Mesh no channels available     0
Incompatible (valid channel) config 0
ARM reset channel check timers 0
SAPM Random Channel           0
ARM Channel from AP's Cache    0
Channel from Config           0
Channel from Sapd Offline      0
--More-- (q) quit (u) pageup (/) search (n) repeat
Interface:wifil
ARM Internal State
-----
Variable                      State
-----
Radar detected                 FALSE
Invalid channel detected       FALSE
Error detected                 FALSE
Noise detected                 FALSE
Channel quality detected       FALSE
40MHz assignment              FALSE
80MHz assignment               FALSE
160MHz assignment              FALSE
80+80MHz assignment           FALSE
Secondary present              FALSE
Multi-band assignment          FALSE
Using default channel          FALSE
Dynamic bw signatures detected FALSE
ARM Status Counters
-----
Status                          Count
-----
SAP Monitor No Mode Aware      0
Null current channel           0
40MHz Intol Detected           0
Hang Detected                   0
Hang Cleared                    0
ARM Disable/Maintain           0
ARM in Backoff                  0

```

```

Client Aware                                0
ARM Clean Channel                           0
ARM Min Scans                               0
ARM No Min Intf Channel                     0
ARM 40M No Min Intf Channel                 0
ARM 80M No Min Intf Channel                 0
ARM 160M No Min Intf Channel                0
ARM Active rogue on home channel            0
ARM Delay Channel Change                    0
ARM Channel Checks                          13
ARM Channel Change                          13
ARM Same 80MHz Channel                      0
ARM Auto Bandwidth Mode Detected            0
Mesh no channels available                   0
Incompatible (valid channel) config         0
ARM reset channel check timers              0
SAPM Random Channel                         0
ARM Channel from AP's Cache                  0
Channel from Config                          0
Channel from Sapd Offline                    0

```

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on managed device.

show ap arm virtual-beacon-report

```
show ap arm virtual-beacon-report
  ap-name <name>
  ip-addr <ipaddr>
  ip6-addr <ip6-addr>
  phy-type 80211a|80211b|80211g
```

Description

If the client match feature is enabled, the output of this command displays the virtual beacon report for an AP with a specific IP or MAC address. The managed device sends APs a list of clients that should not be allowed to associate to that AP.

Parameter	Description
ap-name <name>	Name of an AP for which you want to view a virtual beacon report.
ip-addr <ipaddr>	IPv4 address of an AP for which you want to view a virtual beacon report.
ip6-addr <ip6addr>	IPv6 address of an AP for which you want to view a virtual beacon report.
phy-type	Display virtual beacon report data for an AP radio with one of the following phy types: <ul style="list-style-type: none">■ 80211a■ 80211b■ 80211g

Example

```
(host)[node] #show ap arm virtual-beacon-report ap-name 1263-ac
```

```
Interface:wifi0
Rx VBR Reports:683

Client MAC:24:77:03:cf:fa:5c
Dual band:Yes
Active Voice:No
Steerable:Yes
Dual network capable:No
6GHz Capable: No
Current Association:6c:f3:7f:e7:5a:b0

Virtual Beacon Report
-----
AP           Channel  Signal (dBm)  EIRP  Assoc
```



```

--
-----
9c:1c:12:fd:d2:10 60      -76      12
9c:1c:12:fd:d2:00 1       -66      12
9c:1c:12:fe:13:50 52      -73      21
9c:1c:12:fe:0f:d0 52      -74      24
9c:1c:12:fd:f7:b0 44      -49      20
6c:f3:7f:e7:5a:b0 60      -73      12      Y
9c:1c:12:fd:f2:30 60      -69      12
9c:1c:12:fd:f7:a0 1       -55      12
9c:1c:12:fd:f2:20 1       -65      12
9c:1c:12:fe:13:40 1       -68      12

```

The output of this command includes the following parameters:

Column	Description
AP	MAC address of the AP from which the client can detect a signal
Channel	Channel on which the signal was detected
Signal	Signal strength, in dBm, of the probe request received from Client
EIRP	Amount of power transmitted from the AP antennae
Assoc	A "Y" in this field indicates that the client is currently associated to that AP radio

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output of the command was modified to also display 6 GHz capable.
ArubaOS 8.6.0.0	The output will display an interface report for Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap association

```
show ap association
  anyspot
  ap-group <ap-group>
  ap-name <ap-name>
  bssid <bssid>
  channel <channel>
  client-mac <client-mac>
  dormant
    ap-group <ap-group>
    ap-name <ap-name>
    bssid <bssid>
    channel <channel>
    essid <essid>
    remote {[ap-group <ap-group>] | [ap-name <ap-name>] | [bssid <bssid>] |
    [channel <channel>] | [essid <essid>]}
  essid <essid>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  phy <phy>
  remote
    ap-group <ap-group>
    ap-name <ap-name>
    bssid <bssid>
    channel <channel>
    essid <essid>
  voip-only
```

Description

This command shows the AP association table. Use this command to check if user is connected to an AP. This command validates whether the client is associated and indicates the last AP to which it was connected. If the flags column shows an 'A', the client is currently associated with that AP. Alternately, if the client is not currently associated, the AP with the smallest value of association time is the last AP used by the client.

Parameter	Description
anyspot	Shows AP associations for anyspot virtual AP.
ap-group <ap-group>	Shows AP associations for the specified AP group.
ap-name <ap-name>	Shows AP associations for the specified AP name.
bssid <bssid>	Shows AP associations for the specified Basic Service Set Identifier (BSSID). The BSSID is usually the MAC address of an AP.

Parameter	Description
channel <channel>	Shows AP associations for the specified channel.
client-mac <client-mac>	Shows AP associations for the specified MAC address of a client.
dormant	Shows AP associations for the specified dormant station.
ssid <ssid>	Shows AP associations for the specified Extended Service Set Identifier (ESSID). An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, enclose the ESSID in quotation marks.
ip-addr <ip-addr>	Shows AP associations for the specified IP address of an AP.
ip6-addr <ip-addr>	Shows AP association for the specified IPv6 address of an AP.
phy	(For versions prior to ArubaOS 8.9.0.0)Shows AP association for the specified PHY radio type (802.11a, 802.11b or 802.11g) Use the corresponding keywords a , b , or g . (For ArubaOS 8.9.0.0 or later versions)Shows AP association for the specified PHY radio type (2.4 GHz, 5 GHz, or 6 GHz) Use the corresponding keywords 2 , 5 , or 6 .
remote	Shows AP association for bridge mode AP.
voip-only	Shows AP association for VoIP-only clients.

Example

The following example shows the AP association table based on MAC address of the client (For versions prior to ArubaOS 8.9.0.0).

```
(host) #show ap association client-mac 00:1a:1e:aa:bb:cc

(Aruba7008) *[mynode] #show ap association
The phy column shows client's operational capabilities for current
association

Flags: A: Active, B: Band Steerable, H: Hotspot(802.11u) client, K: 802.11K
client, M: Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w
client, V: 80                2.11v BSS trans capable, P: Punctured
preamble, U: HE UL Mu-mimo, O: OWE client, S: SAE client, E: Enterprise
client, m: Agile Multiband client, C: Cellular Data Capable - network
available, c: Cellular Data Capable - network unavailable, p: Pending GSM
activation, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT      : High throughput;          20: 20MHz;   40: 40MHz; t: turbo-
rates (256-QAM)
VHT   : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
HE    : High Efficiency;      80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
<n>ss: <n> spatial streams
```

```

Association Table
-----
Name  bssid          mac          auth  assoc  aid  l-int  essid
     vlan-id  tunnel-id  phy          assoc. time  num  assoc  Flags  Band
steer moves (T/S)  phy_cap
----  -
-----  -
-----  -
-----  -
-----  -
AP515 80:8d:b7:82:32:10 78:4f:43:8b:17:16 y      y      1    10    S06_
MBO 130      0x1001b      a-VHT-80sgi-3ss 7m:51s      1      WAB    0/0
          a-VHT-80sgi-3ss
AP315 84:d4:7e:d2:08:d0 40:9c:28:42:26:d4 y      y      1    20    S06_
MBO 130      0x10027      a-VHT-80sgi-1ss 15s         1      WVAB   0/0
          a-VHT-80sgi-1ss-V

Num Clients:2
Total num of dual-band capable clients:2
Total num of dual-band capable clients in 2.4G band:0
Total num of dual-band capable clients in 5G band:2
Total num of single-band only clients:0

```

The following example shows the AP association table based on name of the AP (For ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap association ap-name hhm-635

The phy column shows client's operational capabilities for current
association

Flags: A: Active, B: Band Steerable, H: Hotspot(802.11u) client, K: 802.11K
client, M: Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w
client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-
mimo, O: OWE client, S: SAE client, E: Enterprise client, m: Agile Multiband
client, C: Cellular Data Capable - network available, c: Cellular Data
Capable - network unavailable, p: Pending GSM activation, T: Individual TWT
client, t: Broadcast TWT client

PHY Details: HT      : High throughput;          20: 20MHz;  40: 40MHz; t: turbo-
rates (256-QAM)
                VHT  : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80:
80MHz + 80MHz
                HE   : High Efficiency;          80: 80MHz; 160: 160MHz; 80p80:
80MHz + 80MHz
                <n>ss: <n> spatial streams

Association Table
-----
Name  bssid          mac          auth  assoc  aid  l-int  essid  vlan-id  tunnel-id  phy
     assoc. time  num  assoc  Flags  Band  steer moves (T/S)  phy_cap
----  -
-----  -
-----  -
-----  -
-----  -
Num Clients:0
Total num of dual-band capable clients:0
Total num of dual-band capable clients in 2.4G band:0

```

```
Total num of dual-band capable clients in 5G band:0
Total num of clients in 6G band:0
Total num of single-band only clients:0
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.
show ap arm client-match history	This command shows the history of AP association changes triggered by the client match feature.
show ap arm client-match summary	This command shows the history of AP association changes triggered by the client match feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none">■ Added 2, 5, and 6 values to denote 2.4 GHz, 5 GHz, and 6 GHz bands respectively for the <code>phy <phy></code> parameter (For ArubaOS 8.9.0.0 or later versions).■ Added 2.4GHz, 5GHZ, and 6GHZ values for <code>phy</code> and <code>phy_cap</code> output parameters (For ArubaOS 8.9.0.0 or later versions).
ArubaOS 8.6.0.0	Command modified.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap assoc-throttle-counters

show ap assoc-throttle-counters

Description

This command shows counters related to association request throttling.

Example

The following example shows counters related to association request throttling:

```
(host) [mynode] #show ap assoc-throttle-counters
```

```
Association Throttle Counters
-----
Counter                               Value
-----
Dropped association requests          0
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap authorization-profile

```
show ap authorization-profile [<profile-name>]
```

Description

This command shows information about AP authorization profiles. The AP authorization profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site.

By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows the user to connect to an unauthorized remote AP via a wired port then enter a corporate username and password. Once a valid user has authorized the AP and the remote AP will be marked as authorized on the network. The remote AP will then download the configuration assigned to that AP by its permanent AP group.

Run this command without the **<profile-name>** option to display the entire AP authorization profile list, including profile status and the number of references to each profile. Include a profile name to display the authorization group defined for that profile.

Parameter	Description
<profile-name>	The name of an existing AP authorization profile.

Examples

The following example lists all AP authorization profiles. The **References** column lists the number of other profiles with references to that authorization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined AP authorization profiles will not have an entry in the **Profile Status** column.

```
(host) #show ap authorization-profile

AP Authorization profile List
-----
Name           References  Profile Status
----           -
Noauthprofile  1
default        2           Predefined (editable)
Total:2
To display the authentication group for an individual profile, include the
<profile> parameter. The example below shows the profile details for the AP
authorization profile Default.
(host) #show ap authorization-profile default

AP Authorization profile "default" (Predefined (editable))
-----
```



```

Parameter          Value
-----
AP authorization group NoAuthApGroup

```

The output of the **show ap authorization** command includes the following parameters:

Column	Description
AP authorization group	Name of a configuration profile to be assigned to the group unauthorized remote APs.

Related Commands

Command	Description
ap authorization-profile	This command defines a temporary configuration profile for remote APs that are not yet authorized on the network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap blacklist-clients / show ap denylist-clients

show ap blacklist-clients / show ap denylist-clients

Description

Show a list of clients that have been denied access.

Use the [stm](#) CLI command to add or remove users from a denylist. Additionally, the **dot1x authentication**, **VPN authentication** and **MAC authentication** profiles allow you to automatically denylist a client if machine authentication fails.

Examples

The output of this command shows that the controller has a single user-defined blocked client.

```
(host)# show ap blacklist-clients/show ap denylist-clients
```

```
Blacklisted/Denylisted Clients
-----
STA          reason          block-time(sec)  remaining time(sec)
---          -
00:1E:37:CB:D4:52  user-defined  45              3555
```

```
(host)# show ap denylist-clients
Denylist Protected
-----
STA  remaining time(sec)
---  -----
```

The output of this command includes the following information:

Column	Description
STA	MAC address of the blacklisted/denylisted client.
reason	The reason that the user was blacklisted. <ul style="list-style-type: none">■ ARP-attack: Blacklisted/Denylisted for an ARP attack.■ user-defined: Blacklisted/Denylisted due to blacklist criteria were defined by the network administrator■ mitm-attack: Blacklisted/Denylisted for a man in the middle (MITM) attack; impersonating a valid enterprise AP.■ gratuitous-ARP-attack: Blacklisted/Denylisted for a gratuitous ARP attack.■ ping-flood: Blacklisted/Denylisted for a ping flood attack.■ session-flood: Blacklisted/Denylisted for a session

Column	Description
	flood attack. <ul style="list-style-type: none"> ■ syn-flood: Blacklisted /Denylisted for a syn flood attack. ■ session-blacklist/denylist: User session was blacklisted/denylisted . ■ IP spoofing: Blacklisted/Denylisted for sending messages using the IP address of a trusted client. ■ ESI-blacklist/denylist: An external virus detection or intrusion detection application or appliance blacklisted/denylisted the client. ■ CP-flood: Blacklisting/Denylisting for flooding with fake AP beacons. ■ UNKNOWN: Blacklist/Denylisting reason unknown.
block-time (sec)	Amount of time the client has been blocked, in seconds.
remaining time(sec)	Amount of time remaining before the client will be allowed access to the network again.

Related Commands

Command	Description
stm add-blacklist-client /add-denylist-client	Manually add clients from a denylist.
stm remove-blacklist-client/remove-denylist-client <macaddr>	Manually remove clients from a denylist.

Command History

Command	Description
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap blacklist-protected / show ap denylist-protected

show ap blacklist-protected / show ap denylist-protected

Description

Show a list of iOS clients that have received a deauth message from the ARM traffic steering feature.

iOS mobile devices such as an iPhone, iPad, or iPod automatically block an SSID if that device receives more than two deauthentication messages within a five-minute period. To protect iOS devices from blacklisting/denylisting an SSID due to repeated traffic steering attempts, ArubaOS limits the number of traffic steering attempts for these devices to no more than one steering attempt every five minutes. Issue the `show ap blacklist-protected / show ap denylist-protected` command to view a list of clients that are protected against further deauthentication actions for a period of time.

This command is used to display the devices that were in the time period where they would be protected against additional blacklistings/denylistings because of the rate limit setting in.

Examples

The output of this command shows that the controller has a single user-defined blocked client.

```
(host) #show ap blacklist-protected
Blacklist Protected
-----
STA                remaining time(sec)
---                -
b4:18:d1:5f:a5:d2  291
```

Starting from ArubaOS 8.9.0.0, the output of the command is displayed as follows:

```
(host) #show ap denylist-protected
Denylist Protected
-----
STA                remaining time(sec)
---                -
b4:18:d1:5f:a5:d2  291
```

The output of this command includes the following information:

Column	Description
STA	MAC address of the blocked client.
remaining time	The amount of time that the client will remain blocked.

Related Commands

Command	Description
stm add-blacklist-client /add-denylist-client	Manually add clients from a denylist.
stm remove-blacklist-client/remove-denylist-client <macaddr>	Manually remove clients from a denylist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap blacklist-time/show ap denylist-time

show ap blacklist-time/show ap denylist-time

Description

This command shows the AP blacklist/denylist time. This command shows the amount of blacklist/denylist time of the STA when it is blacklisted/denylisted in between disconnection and user-timeout.

Example

The following example shows the AP blacklist/denylisttime:

```
(host) [mynode] #show ap blacklist-time/show ap denylist-time  
ap blacklist-time/denylist-time:3600
```

Related Commands

Command	Description
ap ap-blacklist-time / ap ap-denylist-time	This command determines the time, in seconds, for which a client is manually blacklisted/denylist.
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap ble-database

show ap ble-database [long]

Description

This command is used to display AP Beacon (APB) information collected by BLE relay. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
long	This optional parameter is used to display the following additional information, <ul style="list-style-type: none">■ Bank A UI Sta■ Bank B UI Sta

Example

The following command displays AP Beacon (APB) information collected by BLE relay,

```
(host) #show ap ble-database
BLE APB Information
-----
AP Name  AP Group  BLE MAC  BLE Cur. Bank  BLE Opp. Bank  AP Eth MAC  AP IP
Reported at  ConfigID  Status
-----
-----
Total AP BLE devices reported:0
Note:'Status' column indicates whether information received for an AP's
radio is 'Current' (message received in the last 10 minutes)
: or 'OutOfDate' (message received more than last 10 minutes ago and/or AP
might be down).
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Managed Device.

show ap ble-ibeacon-info

```
show ap ble-ibeacon-info
```

Description

This command displays the iBeacon information for all APs with BLE radios that a controller detects. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Example

The following command displays the BLE iBeacon parameter information:

```
(host)[mynode] #show ap ble_ibeacon_info
AP's BLE radio iBeacon parameter
-----
AP Eth MAC          BLE MAC          Major  Minor  UUID
-----
          TX Power          -----
-----
f0:5c:19:c9:c6:8c  f0:5c:19:c9:c6:8d  1000   10    4152554E-F99B-4A3B-86D0-
947070693A78  14
Total AP BLE devices reported:1
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap bss-table

```
show ap bss-table
  ap-name <ap-name>
  bssid <bssid>
  counters
    ap-name <ap-name>
    bssid <bssid>
    essid <essid>
    ip-addr <ip-addr>
    ip6-addr <ip6-addr>
    port <slot/port>
  details
    essid <essid>
    ip-addr <ip-addr>
    ip6-addr <ip6-addr>
    port <slot/port>
  standby
    ap-name <ap-name>
    bssid <bssid>
    details
    ip-addr <ip-addr>
    ip6-addr <ip6-addr>
    port <slot/port>
```

Description

This command shows the Basic Service Set (BSS) table of an AP. To filter this information and view BSS table data for an individual AP or a specific port and slot number, include the **ap-name**, **bssid**, **essid**, **ip-addr**, or **port** keywords.

Parameter	Description
ap-name <ap-name>	Shows the BSS table for the specified AP name.
bssid <bssid>	Shows the BSS table for the specified Basic Service Set Identifier (BSSID) of an AP. The BSSID is usually the MAC address of an AP.
counters	Shows the BSS table of counters for the specified AP.
details	Shows the BSS table with detailed columns.
essid <essid>	Show the BSS table for the specified Extended Service Set Identifier (ESSID) of an AP. An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, enclose the ESSID in quotation marks.
ip-addr <ip-addr>	Shows the BSS table for the specified IP address of an AP.

Parameter	Description
ip6-addr <ip6-addr>	Shows the BSS table for the specified IPv6 address of an AP.
port <slot/port>	Shows the BSS table for the specified port of an AP.
standby	Show the BSS table for the specified AP in standby mode.

Example

The following example shows the BSS table for the active APs.

- For versions prior to ArubaOS 8.9.0.0:

```
(host) [mynode] #show ap bss-table

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-
standard, p-persistent, b-backup, a-always), n-anyspot
Aruba AP BSS Table
-----
bss          ess          port ip          phy    type
ch/EIRP/max-EIRP cur-cl  ap name  in-t(s) tot-t      mtu  acl-state
acl  fm
---          ---          ---- --          ---    ----  -----
-----
9c:1c:12:fd:ec:e0  qa_testing  N/A  172.16.10.20  g-HT  ap    6/19/19
0          204          0          27d:21h:54m:23s  1578  -    58  T
9c:1c:12:fd:ec:e1  qa_testing1 N/A  172.16.10.20  g-HT  ap    6/19/19
0          204          0          27d:21h:54m:23s  1578  -    58  Tn
9c:1c:12:fd:ec:f0  qa_testing  N/A  172.16.10.20  a-VHT ap    36/10/20
2          204          0          27d:21h:54m:23s  1578  -    58  T
9c:1c:12:fd:ec:f1  qa_testing1 N/A  172.16.10.20  a-VHT ap    36/10/20
0          204          0          27d:21h:54m:23s  1578  -    58  Tn

Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:4
Num Associations:2

Flags: K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = OWE
Transition mode OWE BSS; o = OWE Transition mode Open BSS; M = WPA3-SAE
mixed mode BSS; m = Agile Multiband BSS (forces 11k, 11w); c = MBO Cellular
Data Capable BSS
```

- For ArubaOS 8.9.0.0 or 8.10.0.0:

```
(host) [mynode] #show ap bss-table
```

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-backup, a-always), n-anyspot

cluster (cluster role): U-UAC, A-AAC, sU-Standby UAC, sA-Standby AAC

Aruba AP BSS Table

```
-----
bss                ess                port ip                band/ht-mode/bandwidth
ch/EIRP/max-EIRP  type  cur-cl  ap name  in-t(s)  tot-t
-----
84:d4:7e:e6:17:50  9@hbm-535-rtp  N/A    1.1.1.4    5GHz/VHT/80MHz
52E/18.0/23.0      ap    0       qc-225    0         8d:13h:30m:28s
cc:88:c7:41:64:60  8@hbm-635-psk  N/A    10.65.36.220 6GHz/HE/160MHz
37S/15.0/21.8      ap    0       hbm-635    0         8d:12h:44m:31s
mtu  acl-state  acl  fm  flags  cluster  datazone
-----
1300 -          95  T   D      no
1500 -          92  T   DTWx3 no
```

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2

Num Associations:0

Flags: a = Airslice policy; A = Airslice app monitoring; c = MBO Cellular Data Capable BSS; d = Deferred Delete Pending; D = VLAN Discovered; E = Enhanced-open BSS without transition mode; I = Imminent VAP Down; K = 802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS; o = Enhanced-open transition mode open BSS; O = Enhanced-open BSS with transition mode; r = 802.11r Enabled; t = Broadcast TWT Enabled; T = Individual TWT Enabled; W = 802.11W Enabled; x = MBSSID Tx BSS; 3 = WPA3 BSS;

■ For ArubaOS 8.11.0.0 or later versions:

```
(host) [mynode] #show ap bss-table
fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-
standard, p-persistent, b-backup, a-always), n-anyspot
cluster (cluster role): U-UAC, A-AAC, sU-Standby UAC, sA-Standby AAC
Aruba AP BSS Table
-----
bss                ess                port ip                band/ht-
mode/bandwidth ch/EIRP/max-EIRP  type  cur-cl  ap name  in-t(s)
tot-t  mtu  acl-state  acl  fm  flags  cluster  datazone
-----
-
ac:a3:1e:ff:db:d2  N15_WPA3_AES      N/A    10.216.32.93 5GHz/VHT/20MHz
40/16.0/26.2      ap    1       ac:a3:1e:c7:fd:bc 0         27s
1500 -          2    T   TWz3  U   (AAC=10.216.32.9) no
```

```

ac:a3:1e:ff:db:c0 N15_LOCATION_TEST N/A 10.216.32.93 2.4GHz/HT/20MHz
11/4.5/22.5 ap 0 ac:a3:1e:c7:fd:bc 0 9m:27s
1500 - 89 Bs dKT U (AAC=10.216.32.9) no
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Num APs:2
Num Associations:1
Flags: a = Airslice policy; A = Airslice app monitoring; c = MBO
Cellular Data Capable BSS; d = Deferred Delete Pending; D = VLAN Discovered;
E = Enhanced-open BSS without transition mode; I = Imminent VAP Down; K =
802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS;
o = Enhanced-open transition mode open BSS; O = Enhanced-open BSS with
transition mode; r = 802.11r Enabled; t = Broadcast TWT Enabled;
T = Individual TWT Enabled; W = 802.11W Enabled; x = MBSSID Tx BSS; z =
WPA3-AES-CCM128 BSS; Z = WPA3-AES-CCM128 BSS with transition mode;
3 = WPA3 BSS;

```

The output of this command includes the following information:

Column	Description
bss	The AP Basic Service Set Identifier (BSSID). This is usually the MAC address of the AP
ess	The AP Extended Service Set Identifier (ESSID).
port	The slot and port used by the controller, in the format <slot>/<module>/<port>.
ip	IP address of an AP.
phy (For versions prior to ArubaOS 8.9.0.0)	An AP radio type. Possible values are: <ul style="list-style-type: none"> ■ a—802.11a ■ a-HT—802.11a high throughput ■ g— 802.11g ■ g-HT—802.11g high throughput
band/ht-mode/bandwidth (ArubaOS 8.9.0.0 or later versions)	The AP radio type displayed by radio band/throughput type/channel bandwidth. Possible values for each type are as follows: <ul style="list-style-type: none"> ■ band—2.4GHz, 5GHz, or 6GHz ■ ht-mode—HT, VHT, or HE ■ bandwidth—20MHz, 40MHz, 80MHz, 80+80MHz, or 160MHz
ch/EIRP/max-EIRP	Radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.

Column	Description
type	Shows whether the AP is working as an access point (AP) or air monitor (AM).
cur-cl	Current number of clients on the AP.
ap name	Name of the AP.
in-t (s)	Number of seconds that an AP has been inactive.
tot-t	An AP's total active time, in seconds.
mtu	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
acl-state	<p>An ACL can enable or disable an AP during specific time ranges.</p> <ul style="list-style-type: none"> ▪ Disabled: An ACL with time restrictions is currently disabled (so the AP is enabled). ▪ Enabled: An ACL with time restrictions is currently enabled (so the AP is disabled). ▪ This data column will display a dash (-) if no ACLs are currently configured for the AP.
acl	The ACL ID is displayed based on the role set.
fm	<p>Listed below are the forwarding modes available:</p> <ul style="list-style-type: none"> ▪ T-Tunnel ▪ S-Split ▪ D-Decrypt Tunnel ▪ B-Bridge (s-standard, p-persistent, b-backup, a-always) <p>NOTE: If anyspot is enabled for a particular BSSID, then it is represented as n in the Forwarding Mode parameter.</p>
flags	The type of flags available for the AP.
cluster	The cluster name for the AP.
datazone	The name of the datazone.

Related Commands

Command	Description
<code>show aaa debug</code>	This command shows AAA related debug information.

Command History

Release	Modification
ArubaOS 8.11.0.0	The command output was modified to include the following flags: z = WPA3-AES-CCM128 BSS Z = WPA3-AES-CCM128 BSS with transition mode
ArubaOS 8.9.0.0	The command output was modified to include the following: <ul style="list-style-type: none"> Replaced <code>phy</code> parameter with <code>band/ht-mode/bandwidth</code>. Added x and 3 flags.
ArubaOS 8.6.0.0	Command modified.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap bw-report

```
show ap bw-report {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the bandwidth reporting table for a specific AP.

Parameter	Description
ap-name <ap-name>	Show bandwidth data for an AP with a specific name.
bssid <bssid>	Show bandwidth data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
ip-addr <ip-addr>	Show bandwidth data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Examples

The output of the following command shows the Aruba AP bandwidth table for an AP with the IP address 192.0.2.170.

```
show ap bw-report ap-name AP555-0
```

```
Bandwidth report for AP "AP555-0" radio 0
```

```
-----  
Virtual AP  Allocated Share  Actual Share  Offered Load  Delivered Load  
-----  
corp1344-guest      0%      0%      0 kbps  0 kbps  
corp1344-ethersphere-wpa2 0%      0%      0 kbps  0 kbps  
Average Throughput:0 kbps
```

```
Bandwidth report for AP "AP555-0" radio 1
```

```
-----  
Virtual AP  Allocated Share  Actual Share  Offered Load  Delivered Load  
-----  
corp1344-guest      0%      0%      0 kbps  0 kbps  
corp1344-ethersphere-voip 0%      0%      0 kbps  0 kbps  
corp1344-ethersphere-vocera 0%      0%      0 kbps  0 kbps
```

```
Bandwidth report for AP "AP555-0" radio 2
```

```
-----  
Virtual AP  Allocated Share  Actual Share  Offered Load  Delivered Load  
-----
```

```
Average Throughput:0 kbps
```

The output of this command includes the following information for all radios on the AP:

Column	Description
Virtual AP	Name of a Virtual AP
Allocated Share	Maximum percentage of total bandwidth available to that Virtual AP.
Actual Share	Actual percentage of total bandwidth used by a Virtual AP.
Offered Load	Attempted throughput for the Virtual AP, in kbps.
Delivered Load	Actual throughput for the Virtual AP, in kbps. This value may be less than the offered load if the Virtual AP has used all its allocated bandwidth.
Average Throughput	Average throughput for the virtual AP, in kbps.

Related Commands

Command	Description
aaa bandwidth-contract	This command configures a bandwidth contract.
show ap debug bandwidth-management	This command shows bandwidth management information for clients.

Command History

Release	Modification
ArubaOS 8.6.0.0	A new output parameter <code>Bandwidth report for AP "AP-Name" radio 2</code> was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap cellular

```
show ap cellular
  bearer [ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
  cell
  connection-logs
  connection-lte-logs
  operator
  signal
  sim
  stats
  status
  operator
```

Description

This command shows the cellular information for debugging purposes. This includes information on SIM card, network cell, present operator, signal, statistics, status, connection, and LTE logs. Click parameter links to view the corresponding show commands.

Parameter	Description
bearer	Displays the cellular bearer information of the AP.
cell	Shows network cell information.
connection-logs	Shows connection logs information.
connection-lte-logs	Shows LTE connection logs information.
operator	Shows network operator information.
signal	Shows network signal information.
sim	Shows SIM card information.
stats	Shows statistics on data bytes.
status	Shows overall status.

Command History

Release	Modification
ArubaOS 8.11.0.0	The <code>bearer</code> parameter was introduced.
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular bearer

```
ap-name <ap-name>
ip-addr <ip-addr>
ip6-addr <ip6-addr>
```

Description

Displays the cellular bearer information of the AP.

Parameter	Description
ap-name <ap-name>	Displays the dual access point name (APN) details configured on the SIM of an Aruba USB LTE modem.
ip-addr <ip-addr>	Displays the filter on the IP address.
ip6-addr <ip6-addr>	Displays the IPv6 address of the access point.

Example

An example output of the `show ap cellular bearer ap-name` command.

```
(host) [mynode] #show ap cellular bearer ap-name 20:4c:03:0a:12:fc

bearer list
-----
bearer_id  apn      ip_type  ipv4          ipv6
-----
5          ctnet   "IPV4V6" 100.8.105.106 240e:404:2a21:21c7:1:1:cfb4:7187
6          IMS     "IPV4V6" --             240e:505:2a21:3fe9:1:1:cfb4:7467
```

Command History

Release	Modification
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode or enable mode in the managed device.

show ap cellular cell

```
show ap cellular cell
```

Description

This command shows the network cell information for an AP connected to modem. This includes information on network operator, network mode, channel bandwidth and so on.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the network cell information for an AP.

```
(host) [mynode] (config) #show ap cellular cell ap-name 34:8a:12:c7:7c:ec
-----
MCC: Mobile Country Code
MNC: Mobile Network Code
TAC: Tracking Area Code
ECI: E-UTRAN Cell Identifier
PCI: Physical Cell Identifier
EARFCN: E-UTRA Absolute Radio Frequency Channel Number
UARFCN: UTRA Absolute Radio Frequency Channel Number
RSSI: Received Signal Strength Indication
```

RSRP: Reference Signal Received Power
 RSRQ: Reference Signal Received Quality
 SINR: Logarithmic value of SINR. Range: -20~+30. Unit: dB.

 Serving cell

Parameter	Value
Network operator	CHN-UNICOM
Service state	NOCONN
MCC	460
MNC	01
Network mode	FDD LTE
TAC	10F2
ECI	63B50B
PCI	453
EARFCN	1650
BAND	FDD B3
Bandwidth(uplink/downlink)	20/20 MHz
RSSI	-39
RSRP	-65
RSRQ	-5
SINR	25

Neighbour cells (LTE)

Neighbour type	EARFCN	PCI	RSSI	RSRP	RSRQ
intra	1650	453	-39	-65	-5
inter	375	-	-	-	-
inter	350	-	-	-	-
inter	1825	-	-	-	-

Neighbour cells (WCDMA)

UARFCN	PSC	RSCP	ECNO
10688	-	-	-
10663	-	-	-

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular connection-logs

show ap cellular connection-logs

Description

This command shows the connection logs for a USB modem connected to an AP.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the logs for an Aruba USB modem connected to an AP.

```
(host) [mynode] (config) #show ap cellular connection-logs ap-name
20:4c:03:a4:a6:85
[09/17/21 08:55:38] Aruba USB modem detected: Vendor_ID=2626 Product_ID=0512
[09/17/21 08:55:38] Aruba modem driver loaded
[09/17/21 08:55:40] Model: Aruba LTE Firmware Version: EM12GPAR01A20M4G
IMEI: 869710031619467
[09/17/21 08:55:40] simslot: 1
[09/17/21 08:55:54] current network mode is Automatic, changing to 1
[09/17/21 08:55:54] Aruba USB modem is ready
[09/17/21 08:56:13] Setting up data connection...
[09/17/21 08:56:13] ISP is "CHN-UNICOM"
[09/17/21 08:56:21] LTE successful
10.230.220.120 255.255.255.240 2502 10.230.220.121 192.168.254.254
USB Details is queried and updated
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular connection-lte-logs

show ap cellular connection-lte-logs

Description

This command shows the LTE connection logs for a USB modem connected to an AP.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the LTE connection logs.

```
(host) [mynode] (config) #show ap cellular connection-lte-logs ap-name
20:4c:03:a4:a6:85
[09-17_08:56:13:654] WCDMA&LTE_QConnectManager_Linux&Android_V1.1.33
[09-17_08:56:13:654] quectel-CM profile[1] = (null)/(null)/(null)/0, pincode
= (null)
[09-17_08:56:13:654] Find /sys/bus/usb/devices/1-1 idVendor=2626
idProduct=0512
[09-17_08:56:13:654] Find /sys/bus/usb/devices/1-1:1.4/net/ppp0
[09-17_08:56:13:654] Find usbnet_adapter = ppp0
[09-17_08:56:13:654] Find /sys/bus/usb/devices/1-1:1.4/GobiQMI/qcqmio
[09-17_08:56:13:654] Find qmichannel = /dev/qcqmio
[09-17_08:56:13:688] Get clientWDS = 11
[09-17_08:56:13:752] Get clientWDS = 12
[09-17_08:56:13:816] Get clientDMS = 13
[09-17_08:56:13:879] Get clientNAS = 24
[09-17_08:56:13:943] Get clientUIM = 25
[09-17_08:56:14:007] Get clientWDA = 26
[09-17_08:56:14:071] requestBaseBandVersion EM12GPAR01A20M4G
[09-17_08:56:14:390] requestGetSIMStatus SIMStatus: SIM_READY
[09-17_08:56:14:454] requestGetProfile[1] 3GNET///0
[09-17_08:56:14:545] requestRegistrationState2 MCC: 460, MNC: 1, PS:
Attached, DataCap: LTE
```

```

[09-17_08:56:14:582] requestQueryDataCall IPv4ConnectionStatus: DISCONNECTED
[09-17_08:56:14:774] requestSetupDataCall WdsConnectionIPv4Handle:
0x1db01820
[09-17_08:56:14:965] requestSetupDataCall WdsConnectionIPv6Handle:
0x1e115e10
[09-17_08:56:15:157] requestQueryDataCall IPv4ConnectionStatus: CONNECTED
[09-17_08:56:15:221] requestQueryDataCall IPv6ConnectionStatus: CONNECTED
[09-17_08:56:15:349] Using interface ppp0
[09-17_08:56:15:349] local IP address 10.230.220.120
[09-17_08:56:15:349] remote IP address 10.230.220.121
[09-17_08:56:15:349] primary DNS address 123.123.123.123
[09-17_08:56:15:349] secondary DNS address 123.123.123.124
[09-17_08:56:15:349] ifconfig ppp0 up
[09-17_08:56:15:361] restarting udhcpc on ppp0
[09-17_08:56:21:959] ip -6 address flush dev ppp0
[09-17_08:56:21:970] ip -6 address add
2408:8406:2502:e4b9:e1f8:6966:3c15:cce1/64 dev ppp0
[09-17_08:56:21:983] ip -6 route add default dev ppp0
[09-17_08:56:37:074] Set mtu to 1500

```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular operator

show ap cellular operator

Description

This command shows the network operator information.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.

Parameter	Description
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows information on the network operator for an AP.

```
(host) [mynode] (config) #show ap cellular operator ap-name
20:4c:03:a4:a6:85
Operator list
-----
state      plmn    long name      short name     access technology
-----
current(*) 46001   CHN-UNICOM     UNICOM         E-UTRAN
available  46001   CHN-UNICOM     UNICOM         UTRAN
forbidden  46000   CHINA MOBILE   CMCC           E-UTRAN
forbidden  46011   CHN-CT         CT             E-UTRAN
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular signal

```
show ap cellular signal
```

Description

This command shows the cellular signal information.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the signal information for an Aruba USB modem connected to an AP.

```
(host) [mynode] (config) #show ap cellular signal ap-name 20:4c:03:a4:a6:85
-----
RSRP: Reference Signal Received Power
RSRQ: Reference Signal Received Quality
SINR: Logarithmic value of SINR. Range: -20~+30. Unit: dB.
RSSI: Received Signal Strength Indication
RSCP: Received Signal Code Power
-----

Cellular signal
-----
RSRP  RSRQ  SINR  RSSI (dBm)  RSSI
-----  -----  -----
-65   -5     25    -39         31
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular sim

```
show ap cellular sim
```

Description

This command shows information on the SIM card of a USB modem.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the SIM card information for an Aruba USB modem connected to an AP.

```
(host) [mynode] (config) #show ap cellular sim ap-name 20:4c:03:a4:a6:85
SIM card information
-----
Parameter  Value
-----
Slot       1
Inserted   YES
ICCID      89860121801357984943
IMSI       460010730306324
Carrier     CHN-UNICOM
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular stats

```
show ap cellular stats
```

Description

This command shows statistics on the transmitted and received data bytes of a USB modem.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the statistics of data bytes for an Aruba USB modem connected to an AP.

```
(host) [mynode] (config) #show ap cellular stats ap-name 20:4c:03:a4:a6:85
Cellular statistics
-----
Counter                Value
-----
Total tx bytes         6949
Total rx bytes         8173
Tx bytes since connected 6949
Rx bytes since connected 8173
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ap cellular status

```
show ap cellular status
```

Description

This command shows the overall status of a USB modem.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following example shows the status of an Aruba USB modem connected to an AP.

```
(host) [mynode] (config) #show ap cellular status ap-name 20:4c:03:a4:a6:85
USB Modem Information
-----
Parameter Value
-----
Manufacturer Linux
Product xHCI Host Controller
Serial Number xhci-hcd.0
Driver hub
Vendor ID 1d6b
Product ID 0003
Manufacturer Linux
Product Generic Platform OHCI controller
Serial Number ohci-platform.1
Driver hub
Vendor ID 1d6b
Product ID 0001
Manufacturer Linux
Product Generic Platform OHCI controller
Serial Number ohci-platform.0
Driver hub
Vendor ID 1d6b
Product ID 0001
Manufacturer Quectel
Product EM12-G
Serial Number 0123456789ABCDEF
Driver GobiNet
Vendor ID 2c7c
Product ID 0512
Model Quectel EM12
Firmware Version EM12GPAR01A20M4G
IMEI 869710030743003
GPS Status DISABLE
GPS Latitude Not Available
GPS Longitude Not Available
Cellular Link Status
-----
```

```
Parameter Value
-----
PS service Detached
Network status No Service
```

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.


```
trail-info
status
```

Description

This command shows client specific information. Click parameter links to view the corresponding show commands.

Parameter	Description
trail-info	Shows trail information of wireless client.
status	Shows the current status of a specific client.

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap client trail-info

```
show ap client trail-info [<client-mac>]
```

Description

Use this command to show client activity for debugging purposes. This information includes client activity history and roaming, including reasons for client deauthentication, and any alerts or errors encountered by that client. Without arguments, the table gives the last entry for a number of clients - limited by buffer space. Include the optional `<client-mac>` parameter to show additional details for that specific client.

Client-trail information may be available for clients that are no longer active, as the controller saves a limited amount of client data in a buffer. The maximum number of clients for which trail information is saved is determined by is determined by the controller platform. Each controller saves client trail information for twice the number of active clients supported by that controller platform.

Parameter	Description
<code><client-mac></code>	MAC address of the client.

Examples

The following example shows client-trail information for all clients associated with the controller.

```
(host) #show ap client trail-info

Client Trail Info
-----
MAC          BSSID          ESSID  AP-name  VLAN  Deauth-
reason      Alert
-----
---
00:11:22:33:44:55  00:0b:86:11:22:33  corp   ap1      10    AP-Down
Auth-failure
00:12:32:43:54:65  00:0b:86:11:22:34  corp   ap2      10    AP-Down
Auth-failure
00:31:42:53:64:75  00:0b:86:11:22:35  corp   ap3      10    AP-Down
Auth-failure

This example shows client-trail information for a specific user that
includes information about AP alerts and mobility trails.
(host) #show ap client trail-info 00:11:22:33:44:55
MAC          BSSID          ESSID  AP-name  VLAN  Deauth-
reason      Alert
-----
---
```

```

00:11:22:33:44:55  00:0b:86:11:22:33  corp  ap1  10  AP-down
  Auth-failure
Death Reason
Reason              Timestamp
-----
AP-Down            Apr-12-2013 08:12:34
Alert
Reason              Timestamp
-----
Auth-Failure       Apr-10-2013 03:45:11
Mobility Trail
AP-name            BSSID              ESSID              Timestamp
-----
Ap1                00:0b:86:11:11:11  corp               Apr-10-2013 03:45:11
AP2                00:0b:86:22:22:22  abc                Apr-10-2013 03:45:11

```

The output of these commands include the following information:

Column	Description
MAC	MAC address of the client
BSSID	BSSID of the client
ESSID	ESSID to which the client associated
AP-name	Name of the AP to which the client associated
VLAN	VLAN ID of the VLAN to which the client associated.
Death-reason	Reason why the client was deauthorized.
Alert	Reason why alerts were triggered by the client
Timestamp	If you include the optional <client-mac> parameter, the output will include a timestamp that indicates the time each alert or deauthorization was triggered.
Mobility-Trail	If you include the optional <client-mac> parameter, the output will include the AP name, BSSID and ESSID of the APs to which the client connected, as well as a timestamp showing when the connections were initiated.

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap client status

show ap client status <client-mac>

Description

Shows the current status of a specific client.

Parameter	Description
<client-mac>	MAC address of a client

Examples

The output of the command shows the status of an individual client in the STA (station) table.

```
(host) #show ap client status 00:13:fd:42:32:38

STA Table
-----
bssid          auth  assoc  aid  l-int  essid      vlan-id  tunnel-id
-----
00:1a:1e:a3:02:c9  y    y      7   10    corp-wpa2  65      0x10c0
State Hash Table
-----
bssid          state      reason
-----
00:1a:1e:a3:02:c9  auth-assoc  0
```

The output of this command includes the following information:

Column	Description
bssid	Basic Service Set ID (BSSID) of the client.
auth	This column displays a y if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an n .
assoc	This column displays a y if the AP has been configured for 802.11 association frame types. Otherwise, it displays an n .
aid	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.

Column	Description
l-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Extended Service Set ID (ESSID) of the client.
vlan-id	VLAN ID of the VLAN used by the client.
tunnel-id	Identification number for the tunnel.
state	If the client has been both authorized and associated, this data column will display auth-assoc . If the client has only been authorized, this data column will display auth .
Reason	If the client failed to authenticate, this data column lists the reason code for 802.11 authentication failure.

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap cluster-tech-support

```
show ap cluster-tech-support {ap-name <ap-name>} [<filename>]
```

Description

This command shows cluster information of an AP.

Parameter	Description
ap-name <ap-name>	Shows cluster information of an AP for specified AP name.
<filename>	Stores output in specified filename.

Example

The following example shows cluster information for an AP named ap-205:

```
(host) [mynode] #show ap cluster-tech-support ap-name ap-205

Jul  1 23:05:01|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:06:01|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:07:02|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:08:02|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:09:02|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:10:02|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
Jul  1 23:11:02|---:---:---:---:---:---|---.---.---.---|AMON|send_ap_amp_
payload:139|mgmt-servers:1, STA hash table enties:0, AGR table enties:0
```

Related Commands

Command	Description
show cluster-tech-support	This command displays cluster-related information in relation to the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap config

```
show ap config {ap-group <ap-group>}|{ap-name <ap-name>}|{ssid <ssid>}
```

Description

Show a large list of configuration settings for an ap-group or an individual AP.

Parameter	Description
ap-group <ap-group>	Display configuration settings for an AP group.
ap-name <ap-name>	Display configuration settings for an AP with a specific name.
ssid <ssid>	Display configuration settings for an AP with a specific ESSID. An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.

Examples

The following example shows just some of the configuration settings displayed in the output of this command (For versions prior to ArubaOS 8.9.0.0).

```
show ap config ap-group apgroup14
-----
Parameter                               802.11g      802.11a
Source
-----
--
LMS IP                                   N/A          N/A          ap
system-profile "default"
Backup LMS IP                             N/A          N/A          ap
system-profile "default"
LMS Preemption                             Disabled     Disabled     ap
system-profile "default"
LMS Hold-down Period                       600 sec     600 sec     ap
system-profile "default"
Master/Conductor controller IP address      N/A          N/A
  ap system-profile "default"
RF Band                                     g            g            ap
system-profile "default"
Double Encrypt                             Disabled     Disabled     ap
system-profile "default"
Native VLAN ID                             1           1           ap
system-profile "default"
SAP MTU                                     N/A          N/A          ap
system-profile "default"
Bootstrap threshold                         8           8           ap
system-profile "default"
```

```

Request Retry Interval          10 sec          10 sec          ap
system-profile "default"
Maximum Request Retries        10              10              ap
system-profile "default"
Keepalive Interval             60 sec          60 sec          ap
system-profile "default"
Dump Server                     N/A             N/A             ap
system-profile "default"
Telnet                          Disabled         Disabled         ap
system-profile "default"
FIPS enable                     Disabled         Disabled         ap
system-profile "default"
SNMP sysContact                N/A             N/A             ap
system-profile "default"
RFprotect Server IP            N/A             N/A             ap
system-profile "default"
RFprotect Backup Server IP     N/A             N/A             ap
system-profile "default"
AeroScout RTLS Server          N/A             N/A             ap
system-profile "default"
RTLS Server configuration      N/A             N/A             ap
system-profile "default"
Remote-AP DHCP Server VLAN     N/A             N/A             ap
system-profile "default"
Remote-AP DHCP Server Id       192.168.11.1    192.168.11.1    ap
system-profile "default"
Remote-AP DHCP Default Router  192.168.11.1    192.168.11.1    ap
system-profile "default"
Remote-AP DHCP Pool Start      192.168.11.2    192.168.11.2    ap
system-profile "default"
Remote-AP DHCP Pool End        192.168.11.254  192.168.11.254  ap
system-profile "default"
Remote-AP DHCP Pool Netmask    255.255.255.0   255.255.255.0   ap
system-profile "default"
Remote-AP DHCP Lease Time      0 days          0 days          ap
system-profile "default"
Heartbeat DSCP                 0               0               ap
system-profile "default"
Session ACL                    N/A             N/A             ap
system-profile "default"
Image URL                      N/A             N/A             ap
system-profile "default"
Maintenance Mode               Disabled         Disabled         ap
system-profile "default"
...

```

The example output below shows the configuration settings displayed in the output of this command for AP-555 access point,

```

show ap config ap-group apgroup14
-----
Parameter          802.11g          802.11a
802.11a-secondary

```

```

-----
-----
Source
-----

```

The following example shows just some of the configuration settings displayed in the output of this command (ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap config ap-name hhm-635

Configuration for AP name "hhm-635" AP group "hhm-635"
-----
Parameter
2.4GHz secondary          5GHz 6GHz          5GHz-Source
-----
-----
RF Band
6GHz          6GHz          6GHz          6GHz
"sys-635"          ap system-profile
Recovery Mode
auto          auto          auto          auto
"sys-635"          ap system-profile
RF Band for AM mode scanning
all          all          all          all
"sys-635"          ap system-profile
Native VLAN ID
1          1          1          1
"sys-635"          ap system-profile
WIDS AMPDU Optimization
Enabled          Enabled          Enabled          Enabled
"sys-635"          ap system-profile
Tunnel Heartbeat Interval
1          1          1          1
"sys-635"          ap system-profile
Session ACL
ap-uplink-acl          ap-uplink-acl          ap-uplink-acl
acl          ap-uplink-acl          ap system-profile
"sys-635"
SNMP sysContact
N/A          N/A          N/A          N/A
"sys-635"          ap system-profile
LED operating mode (11n/11ac APs only)
normal          normal          normal
"sys-635"          ap system-profile

```

LED override		Disabled	Disabled
Disabled	Disabled		ap system-profile
"sys-635"			
Driver log level		warnings	warnings
warnings	warnings		ap system-profile
"sys-635"			
Console log level		emergencies	
emergencies		emergencies	ap system-
profile "sys-635"			
SAP MTU		N/A	N/A
N/A	N/A		ap system-profile
"sys-635"			
RAP MTU		1300 bytes	1300 bytes
1300 bytes	1300 bytes		ap system-profile
"sys-635"			
LMS IP		N/A	N/A
N/A	N/A		ap system-profile
"sys-635"			
Backup LMS IP		N/A	N/A
N/A	N/A		ap system-profile
"sys-635"			

The output of this command includes the following parameters.

Column	Description
LMS IP	The IPv4 address of the LMS - the Aruba managed device which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
LMS IPv6	The IPv6 address of the LMS - the Aruba managed device which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
Backup LMS IP	For networks with multiple managed devices, this parameter displays the IPv4 address of a backup to the IP address specified with the lms-ip parameter.

Column	Description
Backup LMS IP	For networks with multiple managed devices, this parameter displays the IPv6 address of a backup to the IP address specified with the lms-ip parameter.
LMS Preemption	When this parameter is enabled, the LMS automatically reverts to the primary LMS IP address when it becomes available.
LMS Hold-down Period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.
Number of IPsec retries	Shows the number of times the AP will attempt to recreate an IPsec tunnel with Mobility Conductor before the AP will reboot. The supported range is 0-1000 retries, and the default value is 360. A value of 0 disables the reboot.
LED operation mode	The operating mode for the LEDs (11n APs only) <ul style="list-style-type: none"> ■ normal: Normal mode ■ off: All LEDs off
Master/Conductor controller IP address	For networks with multiple managed devices, this parameter displays the IP address of Mobility Conductor.
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: <ul style="list-style-type: none"> ■ g = 2.4 GHz ■ a = 5 GHz
Double Encrypt	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).

Column	Description
SAP MTU	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP reboots. On the managed device, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Request Retry Interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.
Maximum Request Retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either reboots or tries the IP address specified by the backup LMS IP address (if configured).
Keepalive Interval	Time, in seconds, between keepalive messages from the AP
Dump Server	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
Telnet	Reports whether telnet access the AP is enabled or disabled.
SNMP sysContact	SNMP system contact information.
AeroScout RTLS Server	Displays whether or not the AP will send RFID tag information to an AeroScout RTLS server.
RTLS Server configuration	Displays whether or not the AP will send RFID tag information to an RTLS server.
Remote-AP DHCP Server VLAN	Shows the VLAN ID of the remote-AP DHCP server used when the managed device is unreachable.

Column	Description
Remote-AP DHCP Server Id	Shows the IP Address of the DHCP DNS Server.
Remote-AP DHCP Default Router	Shows the IP Address of the DHCP Default Router.
Remote-AP DHCP Pool Start	Shows the IP Address used as start of DHCP Pool.
Remote-AP DHCP Pool End	Shows the IP Address used as end of DHCP Pool.
Remote-AP DHCP Pool Netmask	Shows the netmask of DHCP Pool.
Remote-AP DHCP Lease Time	Shows the length of leases, in days (0 means infinite).
Remote-AP uplink total bandwidth	This is the total reserved uplink bandwidth (in Kilobits per second)
Remote-AP bw reservation	Session ACLs with uplink bandwidth reservation in kilobits per second. You can specify up to three session ACLs to reserve uplink bandwidth.
Heartbeat DSCP	DSCP value of AP heartbeats (0-63).
Session ACL	Shows the ACL applied on the uplink of a remote AP.
Maintenance Mode	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to NMS systems or network operations centers when deploying, maintaining, or upgrading the network. The managed device still generates debug syslog messages if debug logging is enabled.
Remote-AP Local Network Access	Enable or disable local network access across VLANs in a Remote-AP.
Radio enable	Shows if the AP's radio is enabled or disabled.
Mode	Shows the operating modes for the AP. <ul style="list-style-type: none"> ■ ap-mode: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. ■ am-mode: Device behaves as an

Column	Description
	<p>AM to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.</p> <ul style="list-style-type: none"> ■ spectrum-mode: Device behaves as a spectrum monitor, sending spectrum analysis data to the managed device. Spectrum monitors do not serve clients.
High throughput enable (radio)	Shows if high-throughput (802.11n) features on the 2.4 GHz frequency band are enabled or disabled.
Channel	Shows the channel number for the AP's 802.11a or 802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.
Transmit EIRP	Shows the current transmission power level.
Advertise 802.11d and 802.11h Capabilities	This column reports whether or not the AP will advertise its 802.11d (Country Information) and 802.11h (TPC) capabilities.
TPC Power	The transmit power advertised in the TPC IE of beacons and probe responses. Range: 0-51 dBm
Spectrum Load Balancing	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the managed device is responding to the wireless clients' probe requests.

Column	Description
	<p>If enabled, the managed device compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.</p>
<p>Spectrum Load Balancing mode</p>	<p>Spectrum Load Balancing Mode allows control over how to balance clients. Select one of the following options:</p> <ul style="list-style-type: none"> ■ channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ radio: Radio-based load-balancing balances clients across APs
<p>Spectrum load balancing update interval</p>	<p>This value determines how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.</p>
<p>Advertised regulatory max EIRP</p>	<p>A cap for an radio's maximum EIRP. Even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.</p>
<p>Spectrum load balancing domain</p>	<p>Define a spectrum load balancing domain to manually create RF neighborhoods.</p> <p>This option creates RF neighborhood information for networks that have disabled ARM scanning and channel assignment.</p> <ul style="list-style-type: none"> ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is <i>not</i> defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain <i>is/also</i> defined, AP radios belonging to the same spectrum

Column	Description
	<p>load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.</p>
<p>Rx sensitivity tuning based channel reuse</p>	<p>The channel reuse feature can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.)</p> <ul style="list-style-type: none"> ■ Static mode: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ Dynamic mode: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ Disable mode: This mode does not support the tuning of the CCA Detect Threshold.
<p>Rx sensitivity threshold</p>	<p>RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold</p>
<p>Non 802.11a interference Immunity</p>	<p>The value for 802.11 Interference Immunity. This parameter sets the interference immunity on the 2.4 GHz band.</p>

Column	Description
	<p>The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferes (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range.</p> <p>The levels for this parameter are:</p> <ul style="list-style-type: none"> ■ Level-0: no ANI adaptation. ■ Level-1: noise immunity only. ■ Level-2: noise and spur immunity. This is the default setting ■ Level-3: level 2 and weak OFDM immunity. ■ Level-4: level 3 and FIR immunity. ■ Level-5: disable PHY reporting.
Enable CSA	Displays whether or not the AP has enabled CSAs for 802.11h.
CSA Count	Number of channel switch announcements that must be sent before the AP will switch to a new channel.
Management Frame Throttle interval	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero rate limiting is disabled for this AP.
Management Frame Throttle Limit	Maximum number of management frames that can come from this radio in each throttle interval.
ARM/WIDS Override	Shows if ARM and Wireless IDS functions are enabled or disabled. If a radio is configured to operate in AM mode, then these functions are always enabled, regardless of this option.
Protection for 802.11b Clients	Displays whether or not protection for 802.11b clients is enabled or disabled.

Column	Description
Maximum Distance	<p>Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16 km.</p> <p>The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 2.4 GHz frequency band radio:</p> <ul style="list-style-type: none"> ■ 20 MHz mode: 54 km ■ 40 MHz mode: 24 km <p>If you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600 m will use default settings.</p>
Spectrum Monitoring	<p>When this parameter is enabled, it turns an AP in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.</p>
Assignment	<p>Displays whether or not ARM channel and power assignment has been enabled or disabled.</p>
Allowed bands for 40MHz channels	<p>Forty MHz channels may be used on the specified radio bands (802.11a or 802.11g).</p>
Client Aware	<p>Shows if the client aware feature has been enabled or disabled for this AP. If enabled, AP will not change channels when there are active clients.</p>
Max Tx Power	<p>Maximum transmission power for this AP, in dBm.</p>
Min Tx Power	<p>Minimum transmission power for this AP, in dBm.</p>
Multi Band Scan	<p>Shows if the multi-band scan feature has been enabled or disabled on this AP. If enabled, single-radio APs will try to scan across bands for Rogue AP detection.</p>

Column	Description
Rogue AP Aware	Shows if the rogue AP awareness feature has been enabled or disabled on this AP. If enabled, the AP will try to contain off-channel Rogue APs.
Scan Interval	This parameter indicates, in seconds, how often the AP will leave its current channel to scan other channels in the band if scanning is enabled.
Active Scan	<p>Displays whether or not the active scan feature is enabled.</p> <p>NOTE: This option elicits more information from nearby APs, but also creates additional management traffic on the network. Active Scan is disabled by default, and should <i>not be enabled</i> except under the direct supervision of Aruba Support.</p>
Scanning	<p>Shows if scanning is enabled or disabled for this AP. If this option is disabled, the following other options will also be disabled:</p> <ul style="list-style-type: none"> ■ Multi Band Scan ■ Rogue AP Aware ■ Voip Aware Scan ■ Power Save Scan
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, VoIP Aware Scan should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that Scanning is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. Default: enabled

Column	Description
Ideal Coverage Index	The Aruba coverage index metric is a weighted calculation based on the RF coverage for all Aruba APs and neighboring APs on a specified channel. The Ideal Coverage Index specifies the ideal coverage that an AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Acceptable Coverage Index	For multi-band implementations, the Acceptable Coverage Index specifies the minimal coverage an AP it should achieve on its channel. The denser the AP deployment, the lower this value should be.
Free Channel Index	The current free channel index value. The Aruba Interference index metric measures interference for a specified channel and its surrounding channels. This value is calculated and weighted for all APs on those channels (including 3rd-party APs). An AP will only move to a new channel if the new channel has a lower interference index value than the current channel. Free Channel Index specifies the required difference between the two interference index values before the AP moves to the new channel. The lower this value, the more likely it is that the AP will move to the new channel.
Backoff Time	After an AP changes channel or power settings, it waits for this backoff time interval before it asks for a new channel or power setting.
Error Rate Threshold	The minimum percentage of PHY errors and MAC errors in the channel that will trigger a channel change.
Error Rate Wait Time	Minimum time in seconds the error rate on the AP has to exceed its defined error rate threshold before it triggers a channel change.
Noise Threshold	Maximum level of noise in a channel that triggers a channel change.

Column	Description
Noise Wait Time	Minimum time in seconds the noise level has to exceed the Noise Threshold before it triggers a channel change on the AP.
Minimum Scan Time	Minimum number of times a channel must be scanned before it is considered for assignment. Best practices are to configure a Minimum Scan Time between 1-20 scans.
Load aware Scan Threshold	The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.
Mode Aware Arm	Shows if the mode-aware ARM feature has been enabled or disabled for this AP. If enabled, ARM will turn the AP into an AMs if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
Scan mode	Identifies the scan mode for the AP. <ul style="list-style-type: none"> ■ all-reg-domain: The AP scans channels within all regulatory domains. This is the default setting. ■ reg-domain: Limit the AP scans to just the regulatory domain for that AP.
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.

Column	Description
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
SSID enable	Shows if the SSID is enabled or disabled
ESSID	Name that uniquely identifies the Extended SSID.
Encryption	Encryption type used on this AP.
DTIM Interval	Shows the interval, in milliseconds, between the sending of DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed.
Basic Rates	Lists supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses from this AP.
Transmit Rates	Lists 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Max Transmit Attempts	Maximum number of retries allowed for the AP to send a frame
RTS Threshold	Wireless clients transmitting frames larger than this threshold must issue RTS and wait for the AP to respond with CTS. This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.

Column	Description
Short Preamble	Shows if a short preamble for 802.11b/g radios is enabled or disabled for this AP. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.
Max Associations	Maximum number of wireless clients allowed to associate to the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	Shows if Wireless Multimedia (WMM) UAPSD powersave is enabled or disabled.
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity timeout threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
902il Compatibility Mode	Shows if 902il compatibility mode is enabled or disabled. (This parameter only needs to be enabled for APs with associated clients using NTT DoCoMo 902iL phones.)
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is enabled or disabled.

Column	Description
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the controller sends the 802.11 probe responses
Disable Probe Retry	If disabled, the AP will not resend probes if it does not get a response.
Battery Boost	Shows if the battery boost feature is enabled or disabled for the AP. If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life
Drop Broadcast and Multicast	If this feature is enabled on an AP, it drops all downstream broadcast or multicast traffic to increase battery life.
WEP Key 1	Displays the static WEP key (1 of 4).
WEP Key 2	Displays the static WEP key (2 of 4).
WEP Key 3	Displays the static WEP key (3 of 4).
WEP Key 4	Displays the static WEP key (4 of 4).
WEP Transmit Key Index	Displays the key index that specifies which static WEP key is to be used.
WPA Hexkey	Displays the WPA PSK.
WPA Passphrase	Displays the WPA passphrase with which the AP generates a PSK.

Column	Description
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
Rate Optimization for delivering EAPOL frames	Shows if the AP has enabled or disabled rate optimization for delivering EAPOL frames.
Strict Spectralink Voice Protocol (SVP)	Shows if strict SVP is enabled or disabled.
802.11g Beacon Rate	Sets the beacon rate for 802.11g for APs use a DAS. Using this parameter in normal operation may cause connectivity problems.
802.11a Beacon Rate	Sets the beacon rate for 802.11a for APs use a DAS. Using this parameter in normal operation may cause connectivity problems.
Advertise QBSS Load IE	Shows if the AP has enabled or disabled the advertising of QBSS in the load IE.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MPDU aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be received on the AP's high-throughput SSID.

Column	Description
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPU within an aggregate MDPU, in microseconds.
Supported MCS set	Comma-separated list of MCS values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 20 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 20 MHz mode of operation.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.
Maximum number of spatial stream usable for STBC transmission	Controls the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)
Minimum number of spatial stream usable for STBC transmission	Controls the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.)
Legacy stations	Shows if the AP has enabled or disabled the legacy stations option, which controls whether or not legacy (non-HT) stations are allowed to associate with the AP's SSID. By default, legacy stations are allowed to associate. NOTE: This setting has no effect on a BSS in which HT support is not available.
Allow weak encryption	Shows if the AP has enabled or disabled the weak encryption option.

Column	Description
	The use of TKIP or WEP for unicast traffic forces the use of legacy transmissions rates. Disabling this mode prevents the association of stations using TKIP or WEP for unicast traffic. This mode is disabled by default.
Virtual AP enable	WLAN profiles configure WLANs in the form of virtual AP profiles. This parameter shows if the AP has enabled or disabled virtual APs.
Allowed band	Shows the band(s) on which to use the virtual AP: <ul style="list-style-type: none"> ■ a—802.11a band only (5 GHz) ■ g—802.11b/g band only (2.4 GHz) ■ all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)
VLAN	Shows the VLAN(s) into which users are placed in order to obtain an IP address.
Forward mode	Shows the current forward mode (tunnel, bridge, split-tunnel, or decrypt-tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the controller using GRE, bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic. When the controller sends traffic to a client, the controller sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client. Only 802.1X authentication is supported when configuring bridge or split tunnel mode.
Deny time range	Shows the time range for which the AP will deny access for a virtual AP.

Column	Description
Mobile IP	Shows if IP mobility has been enabled or disabled for the virtual AP.
HA Discovery on-association	<p>If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practice is to keep this parameter disabled as it increases IP mobility control traffic between controllers in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients.</p> <p>NOTE: <code>ha-disc-onassoc</code> parameter works only when IP mobility is enabled and configured on the controller.</p>
DoS Prevention	Shows the status of the Dos Prevention option. If enabled, virtual APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.
Station Blacklisting/Denylisting	Shows if the virtual AP has enabled or disabled detection of DoS attacks, such as ping or SYN floods, that are not spoofed deauth attacks.
Blacklist/Denylist Time	Shows the number of seconds that a client will be quarantined from the network after being blacklisted/denylisted.
Authentication Failure Blacklist/Denylist Time	Shows the time, in seconds, a client is blocked if it fails repeated authentication. If the virtual AP shows a value of 0, a blacklisted/denylisted client is blocked indefinitely.
Fast Roaming	Shows if the AP has enabled or disabled fast roaming.

Column	Description
Strict Compliance	If enabled, the virtual AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
VLAN Mobility	Shows if a virtual AP has enabled or disabled VLAN (Layer-2) mobility
Remote-AP Operation	Shows when the virtual AP operates on a remote AP: <ul style="list-style-type: none"> ■ always—Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ backup—Enables the virtual AP if the remote AP cannot connect to the controller (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ persistent—Permanently enables the virtual AP after the remote AP initially connects to the controller (Bridge Mode only). This option can be used for any (Open/PSK/802.1X) bridge VAPs. ■ standard—Enables the virtual AP when the remote AP connects to the controller. This option can be used for any (bridge/split-tunnel/tunnel/d-tunnel) VAPs.
Convert Broadcast ARP requests to unicast	If this option is enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the show ap active and the show datapath tunnel command. If enabled, the output will display the letter a in the flags column.
Band Steering	Shows if band-steering has been enabled or disabled for a virtual AP.

Column	Description
	<p>ARM's band steering feature encourages dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones.</p> <p>Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40 MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.</p>

Related Commands

Command	Description
ap system-profile	The output of the show ap config command displays the content of the profile settings for an individual AP or AP group. Use the commands displayed in the column to the left to configure these parameters.
rf dot11g-radio-profile	This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.
rf arm-profile	This command configures the Adaptive Radio Management (ARM) profile.
rf ht-radio-profile	This command configures high-throughput AP radio settings. High-throughput features use the IEEE 802.11n standard.
wlan ht-ssid-profile	This command configures a high-throughput SSID profile.
wlan virtual-ap	This command configures a virtual AP profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were made:

Release	Modification
	<ul style="list-style-type: none"> ■ The command output was modified to include 2.4GHz, 5GHz, 5GHz-secondary, and 6GHz parameters (ArubaOS 8.9.0.0 or later versions). ■ All instances of <code>Blacklist</code> and <code>Blacklisting</code> have been replaced with <code>Denylist</code> and <code>Denylisting</code> respectively. ■ All instances of <code>master</code> have been replaced with <code>conductor</code>.
ArubaOS 8.6.0.0	The output parameter <code>802.11a-secondary</code> was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap consolidated-provision info

```
show ap consolidated-provision info
  ap-name <ap-name>
  ip-addr <ip-address>
  ip6-addr <ipv6-address>
```

Description

This command shows the consolidated provision details of an AP.

Parameter	Description
ap-name <ap-name>	Shows consolidated provision information based on the AP name.
ip-addr <ip-address>	Shows consolidated provision information based on the IP address of an AP.
ip6-addr <ipv6-address>	Shows consolidated provision information based on the IPv6 address of an AP.

Examples

The following example shows the consolidated provision details of an AP with name xxxxx-ap-135.

```
(host) #show ap consolidated-provision info ap-name xxxxx-ap-135
ap name: xxxxx-ap-135
ipv4 address type: dynamic
ipv4 address: 10.17.160.247
ipv4 netmask: 255.255.255.0
ipv4 gateway: 10.17.160.2
ipv4 lease: 43200
ipv4 dhcp server: 10.17.160.2
ipv4 dns server: 10.13.6.110, 0.0.0.0
ipv6 address: none
master/ conductor : 10.17.160.4
master/ conductor discover type: Provisioned manually
previous lms: none
lms addrs [0]: 10.17.160.4
```

The output of this command includes the following parameters.

Column	Description
ap name	The name of the AP for which consolidated provisioned information is required.
ipv4 address type	The IPv4 address type of the AP.
ipv4 address	The IPv4 address of the AP.
ipv4 netmask	The IPv4 subnet mask of the AP.
ipv4 gateway	The IPv4 gateway information of the AP.
ipv4 lease	The IPv4 lease information pertaining to the AP.
ipv4 dhcp server	The IPv4 DHCP server of the AP.
ipv4 dns server	The IPv4 DNS server of the AP.
ipv6 address	The IPv6 address of the AP.
master/ conductor	The IP address of the AP's Mobility Conductor.
master/ conductor discover type	The Mobility Conductor discovery (provisioning) type information for the AP
previous lms	The previous LMS IP address of the AP.
lms addr	The LMS IP address of the AP.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap convert-download-log

show ap convert-download-log <number>

Description

This command shows the logs for downloading images from Activate or other server by the AP conversion feature.

Parameter	Description
<number>	The line number from the log.

Example

The following example shows the image downloading logs from Activate server:

```
(host) *[mynode] #show ap convert-download-log

upgrading now
Download file ArubaInstant_Ursa_10.1.0.0_76943
fetching ('/mswitch/bin/wget -T 120 -t 3 --proxy --proxy-user= --proxy-
passwd=***** --no-check-certificate -a /tmp/sapm_download_image.log
http://activate-frm5-cf.arubathena.com/fwfiles/ArubaInstant_Ursa_10.1.0.0_
76943')
--18:44:49-- http://activate-frm5-cf.arubathena.com/fwfiles/ArubaInstant_
Ursa_10.1.0.0_76943
=> `ArubaInstant_Ursa_10.1.0.0_76943'
Resolving activate-frm5-cf.arubathena.com... 99.84.231.84
Connecting to activate-frm5-cf.arubathena.com|99.84.231.84|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17,972,496 (17M) [binary/octet-stream]
 0K ..... 0% 120.79
KB/s
 50K ..... 0% 276.96
KB/s
100K ..... 0% 338.44
KB/s
150K ..... 1% 837.95
KB/s
200K ..... 1% 437.88
KB/s
250K ..... 1% 1.22
MB/s
300K ..... 1% 1.03
MB/s
350K ..... 2% 516.09
KB/s
400K ..... 2% 1.82
MB/s
```

450K	2%	1.92
MB/s			
500K	3%	1.86
MB/s			
550K	3%	544.84
KB/s			
600K	3%	2.37
MB/s			
650K	3%	2.24
MB/s			
700K	4%	3.08
MB/s			
750K	4%	1.60
MB/s			
800K	4%	617.60
KB/s			
850K	5%	3.45
MB/s			
900K	5%	3.49
MB/s			
950K	5%	3.58
MB/s			
1000K	5%	3.82
MB/s			
1050K	6%	3.93
MB/s			
1100K	6%	4.20
MB/s			
1150K	6%	3.90
MB/s			
1200K	7%	608.55
KB/s			
1250K	7%	4.24
MB/s			
1300K	7%	4.45
MB/s			
1350K	7%	3.83
MB/s			
1400K	8%	5.19
MB/s			
.			
.			
.			

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap convert-image-list

show ap convert-image-list

Description

This command shows the list of all available images for converting Campus AP or Remote AP to Instant AP.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the list of available images for AP conversion:

```
(host) [mynode] (config) #show ap convert-image-list

AP Conversion Image list
-----
Image File Name                               Build Info                                     Size
-----
-----
ArubaInstant_Draco_10.1.0.0_76943             ArubaOS version 10.1.0.0-10.1.0.0 for
Draco (jenkins@pr-hpn-cd-build04) (gcc version 5.3.0 (Buildroot 2016.02) )
#76943 SMP Tue Sep 1 04:50:43 PDT 2020
21927936
ArubaInstant_Gemini_10.1.0.0_76943           ArubaOS version 10.1.0.0-10.1.0.0 for
Gemini (jenkins@pr-hpn-cd-build01) (gcc version 5.3.0 (Buildroot 2016.02) )
#76943 SMP Tue Sep 1 05:03:44 PDT 2020
19385916
ArubaInstant_Hercules_10.1.0.0_76943         ArubaOS version 10.1.0.0-10.1.0.0 for
Hercules (jenkins@pr-hpn-cd-build12) (gcc version 4.6.3 20120201
(prerelease) (Linaro GCC 4.6-2012.02) ) #76943 SMP Tue Sep 1 05:18:34 PDT
2020 18898704
ArubaInstant_Lupus_10.1.0.0_76943           ArubaOS version 10.1.0.0-10.1.0.0 for
Lupus (jenkins@pr-hpn-cd-build09) (gcc version 4.8.1) #76943 SMP Tue Sep 1
04:52:45 PDT 2020
18478988
ArubaInstant_Scorpio_10.1.0.0_76943         ArubaOS version 10.1.0.0-10.1.0.0 for
Scorpio (jenkins@pr-hpn-cd-build14) (gcc version 5.3.0) #76943 SMP Tue Sep 1
05:23:49 PDT 2020
23694284
ArubaInstant_Ursa_10.1.0.0_76943           ArubaOS version 10.1.0.0-10.1.0.0 for
Ursa (jenkins@pr-hpn-cd-build15) (gcc version 4.6.3) #76943 SMP Tue Sep 1
05:18:16 PDT 2020
17972496
```

The output of this command includes the following parameters:

Column	Description
Image File Name	The name of the available image file.
Build Info	The version number and other information of the ArubaOS build.
Size	The size of the image file .

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap convert-status-list

```
show ap convert-status-list {page <page>|start <page>}
```

Description

This command shows only the list of APs and their conversion status.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
page <page>	Number of APs to display.
start <page>	Starting AP index.

Example

The following example shows the conversion status of a particular AP image:

```
(host) [mynode] (config) #show ap convert-status-list

AP Image Conversion Status
-----
AP Name          AP Group  AP Mac          AP Serial #  AP IP
AP Type Upgrade State Start Time      End Time      Failure Count
Failure Reason
-----
-----
70:3a:0e:cc:ee:52 default  70:3a:0e:cc:ee:52  CNBQJ0Y0D4   10.65.17.124
335      Updating    2020-10-29 18:49:13      0
```

The output of this command includes the following parameters:

Column	Description
AP Name	Name of the AP selected for conversion.
AP Group	AP group of the AP selected for conversion.
AP Mac	MAC address of the AP.
AP Serial #	Serial number of the AP.

Column	Description
AP IP	IP address of the AP.
AP Type	Type of AP model.
Upgrade State	Current state of the AP's upgrade attempt .
Start Time	Time the AP started upgrading an image.
End Time	Time the AP completed the image upgrade.
Failure Count	Number of times the AP failed to upgrade the new image.
Failure Count	In the event of an image upgrade failure, this column displays the reason for the failure.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap convert-setup-image-log

show ap convert-setup-image-log <number>

Description

This command shows the logs for moving the AP conversion images to the temporary image folder.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<number>	The line number from the log.

Example

The following example shows the logs for moving the AP conversion images:

```
(host) [mynode] (config) #show ap convert-setup-image-log

/mswitch/bin/sapm_setup_iap_images.sh --image-file=/tmp/sapm_download_images
--image-file-is-list=1 --target-folder=/flash/apimages --platform=0
check images listing in the file /tmp/sapm_download_images
image file list:
/tmp/sapm_tmp_imgs/ArubaInstant_Ursa_10.1.0.0_76943
/tmp/sapm_tmp_imgs/ArubaInstant_Draco_10.1.0.0_76943
/tmp/sapm_tmp_imgs/ArubaInstant_Scorpio_10.1.0.0_76943
/tmp/sapm_tmp_imgs/ArubaInstant_Hercules_10.1.0.0_76943
/tmp/sapm_tmp_imgs/ArubaInstant_Gemini_10.1.0.0_76943
/tmp/sapm_tmp_imgs/ArubaInstant_Lupus_10.1.0.0_76943
process file /tmp/sapm_tmp_imgs/ArubaInstant_Ursa_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Ursa_10.1.0.0_76943 to image
folder /tmp/sapm_setup_tmp_image_folder
process file /tmp/sapm_tmp_imgs/ArubaInstant_Draco_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Draco_10.1.0.0_76943 to image
folder /tmp/sapm_setup_tmp_image_folder
process file /tmp/sapm_tmp_imgs/ArubaInstant_Scorpio_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Scorpio_10.1.0.0_76943 to image
folder /tmp/sapm_setup_tmp_image_folder
process file /tmp/sapm_tmp_imgs/ArubaInstant_Hercules_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Hercules_10.1.0.0_76943 to image
folder /tmp/sapm_setup_tmp_image_folder
process file /tmp/sapm_tmp_imgs/ArubaInstant_Gemini_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Gemini_10.1.0.0_76943 to image
folder /tmp/sapm_setup_tmp_image_folder
process file /tmp/sapm_tmp_imgs/ArubaInstant_Lupus_10.1.0.0_76943
move image /tmp/sapm_tmp_imgs/ArubaInstant_Lupus_10.1.0.0_76943 to image
```

```
folder /tmp/sapm_setup_tmp_image_folder  
Running sbfile  
clean folder /tmp/sapm_setup_tmp_image_folder
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap convert-status

```
show ap convert-status {page <page>|start <page>}
```

Description

This command shows the status of AP image conversion operation.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
page <page>	Number of APs to display.
start <page>	Starting AP index.

Example

The following example shows the status of AP image conversion including the AP conversion parameters, and the details of AP meant for conversion:

```
(host) *[mynode] #show ap convert-status

AP Conversion Parameters
-----
Item                               Value
----                               -
Status                             Active
Mode                               Specific APs
Image Source                       Activate
Max Simultaneous Converting        10
current Simultaneous Converting    1
Auto Reboot                        True
Start Time                         2020-10-29 18:49:13
Current Status                     Converting APs

AP Names Listed for Conversion
-----
AP Names
-----
70:3a:0e:cc:ee:52

AP Image Conversion AP Status Summary
-----
AP Image Conversion State  Count
-----
Updating                  1
TOTAL                    1
```

```

AP Image Conversion Status
-----
AP Name          AP Group AP Mac          AP Serial # AP IP
AP Type Upgrade State Start Time      End Time  Failure Count
Failure Reason
-----
-----
70:3a:0e:cc:ee:52 default 70:3a:0e:cc:ee:52 CNBQJ0Y0D4 10.65.17.124
335      Updating      2020-10-29 18:49:13          0

```

The output of this command includes the following parameters:

Column	Description
AP Conversion Parameters	Shows the following conversion parameter values:
Status	Indicates if the conversion feature is enabled (active status) or disabled (inactive status). Displays one of the following values: <ul style="list-style-type: none"> ■ Active ■ Inactive
Mode	Indicates the conversion mode. Displays one of the following values: <ul style="list-style-type: none"> ■ All APs ■ Specific APs
Image Source	Indicates the image source. Displays one of the following values: <ul style="list-style-type: none"> ■ Flash: The image is copied into the controller flash. ■ Image Server: The image is on ftp, tftp, scp, or https server. ■ Activate: The controller obtains the image from Aruba Activate server. This is the recommended value. ■ None: The conversion is not active.
Max Simultaneous Converting	Indicates the number of APs that are allowed for conversion at the same time.
Current Simultaneous Converting	Indicates the number of APs currently getting converted.
Auto Reboot	Indicates whether the AP auto reboots after conversion. Displays one of the following values: <ul style="list-style-type: none"> ■ True ■ False

Column	Description
Start Time	Indicates the starting time of the conversion.
Current Status	Indicates the conversion status. Displays one of the following values: <ul style="list-style-type: none"> ■ Not Start ■ Pre-Validating ■ Pre-Validate Success ■ Pre-Validate Failed ■ Pre-Validate Timeout ■ Activate Connecting ■ Activate Connect Error ■ Downloading Image ■ Download Image Error ■ Download Image Timeout ■ Installing Image Into MD Image Folder ■ Install Image Error ■ Preload Image Is Operating ■ Updating APs ■ Update Done
AP Names Listed for Conversion	Shows the AP name listed for conversion.
AP Image Conversion AP Status Summary	These two columns list the different possible conversion states for APs, and the total number of APs in each state.
AP Image Conversion Status	This section displays the following details for each conversion attempt:
AP Name	Name of the AP selected for conversion.
AP Group	AP group of the AP selected for conversion.
AP Mac	MAC address of the AP.
AP Serial #	Serial number of the AP.
AP IP	IP address of the AP.
AP Type	Type of AP model.
Upgrade State	Current state of the AP's upgrade attempt .
Start Time	Time the AP started upgrading an image.
End Time	Time the AP completed the image upgrade.

Column	Description
Failure Count	Number of times the AP failed to upgrade the new image.
Failure Count	In the event of an image upgrade failure, this column displays the reason for the failure.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap convert-status-summary

show ap convert-status-summary

Description

This command shows the status of AP conversion operation excluding the AP details.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the summary of AP image conversion without the AP details:

```
(host) [mynode] (config) #show ap convert-status-summary

AP Conversion Parameters
-----
Item                               Value
----                               -
Status                             Active
Mode                               Specific APs
Image Source                       Activate
Max Simultaneous Converting        10
current Simultaneous Converting    1
Auto Reboot                        True
Start Time                         2020-10-29 18:49:13
Current Status                     Converting APs

AP Names Listed for Conversion
-----
AP Names
-----
70:3a:0e:cc:ee:52

AP Image Conversion AP Status Summary
-----
AP Image Conversion State  Count
-----
Updating                  1
TOTAL                    1
```

The output of this command includes the following parameters:

Column	Description
	Shows the following conversion parameter values:

Column	Description
AP Conversion Parameters	
Status	<p>Indicates if the conversion feature is enabled (active status) or disabled (inactive status). Displays one of the following values:</p> <ul style="list-style-type: none"> ■ Active ■ Inactive
Mode	<p>Indicates the conversion mode. Displays one of the following values:</p> <ul style="list-style-type: none"> ■ All APs ■ Specific APs
Image Source	<p>Indicates the image source. Displays one of the following values:</p> <ul style="list-style-type: none"> ■ Flash: The image is copied into the controller flash. ■ Image Server: The image is on ftp, tftp, scp, or https server. ■ Activate: The controller obtains the image from Aruba Activate server. This is the recommended value. ■ None: The conversion is not active.
Max Simultaneous Converting	<p>Indicates the number of APs that are allowed for conversion at the same time.</p>
Current Simultaneous Converting	<p>Indicates the number of APs currently getting converted.</p>
Auto Reboot	<p>Indicates whether the AP auto reboots after conversion. Displays one of the following values:</p> <ul style="list-style-type: none"> ■ True ■ False
Start Time	<p>Indicates the starting time of the conversion.</p>
Current Status	<p>Indicates the conversion status. Displays one of the following values:</p> <ul style="list-style-type: none"> ■ Not Start ■ Pre-Validating ■ Pre-Validate Success ■ Pre-Validate Failed ■ Pre-Validate Timeout ■ Activate Connecting ■ Activate Connect Error ■ Downloading Image ■ Download Image Error

Column	Description
	<ul style="list-style-type: none"> ■ Download Image Timeout ■ Installing Image Into MD Image Folder ■ Install Image Error ■ Preload Image Is Operating ■ Updating APs ■ Update Done
AP Names Listed for Conversion	Shows the AP name listed for conversion.
AP Image Conversion AP Status Summary	These two columns list the different possible conversion states for APs, and the total number of APs in each state.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap-crash-transfer

```
show ap-crash-transfer
```

Description

This command displays info for the AP crash transfer feature, which transfers AP coredump files to the controller flash memory if no dumpserver is configured.

The command `ap system-profile <profile> dump-server <server>` specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the `ap-crash-transfer` command to save dump files to the controller flash memory.



If you define a dump server and issue the `ap-crash-server` command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)[mynode] #show ap-crash-transfer
AP Crash Transfer:enabled
AP Crash folder limit:50 MB (non-editable)
```

Related Commands

Command	Description
<code>ap-crash-transfer</code>	This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

show ap database

```
show ap database
  flags <flags>
  group {default|noauthapgroup|<group>}
  inactive {flags|group|indoor|local|long|outdoor|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  indoor {flags|group|inactive|local|long|outdoor|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  local {flags|group|inactive|indoor|long|outdoor|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  long {flags|group|inactive|indoor|local|outdoor|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  outdoor {flags|group|inactive|indoor|local|long|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  page <page> {flags|group|inactive|indoor|local|long|outdoor|sort-by|sort-
direction|start|status|switch|type|unprovisioned|usb}
  sort-by {ap-flags|ap-group|ap-ip|ap-mac|ap-name|ap-serial|ap-
type|fqln|provisioned|status|switch-ip|uptime}
  sort-direction {ascending|descending}
  start <start>
  status {up|down}
  switch <switch-ip-addr>
  type {cap|mesh|rap}
  unprovisioned {flags|group|inactive|indoor|local|long|outdoor|page|sort-by|sort-
direction|start|status|switch|type|usb}
  usb {flags|group|inactive|indoor|local|long|outdoor|page|sort-by|sort-
direction|start|status|switch|type|unprovisioned}
```

Description

This command shows the list of access points in the database. Many of the parameters in this command can be used together to filter a large database of information down to just the AP data you want to see. For example, you can issue the command `show ap database group <group> local status up` to view a list of local APs within a specific AP group that are reporting an **up** status. Include the **sort-by** and **sort-direction** keywords to specify how the data is sorted in the output of this command.

Parameter	Description
<code>flags <flags></code>	Shows only access points with specified flags. NOTE: Starting from ArubaOS 8.11.0.0, all available flags are included in the flags <flags> sub-parameter.
<code>group <group></code>	Shows only access points in specified AP group.
<code>inactive</code>	Shows only local access points with no active BSSIDs or wired AP interfaces.

Parameter	Description
indoor	Shows only indoor access points.
local	Shows only access points connected to this managed device.
long	Shows following additional columns for access points: <ul style="list-style-type: none"> ■ Wired MAC Address, ■ Serial # ■ Port ■ FQLN
outdoor	Shows only outdoor access points.
page <page>	Shows only specified number of access points.
sort-by	Shows access points filtered by following columns: <ul style="list-style-type: none"> ■ ap-flags ■ ap-group ■ ap-ip ■ ap-mac ■ ap-name ■ ap-serial ■ ap-type ■ fqln ■ provisioned ■ status ■ switch-ip ■ uptime
sort-direction	Shows access points in sorted in following sequence: <ul style="list-style-type: none"> ■ ascending ■ descending
start <start>	Shows access points from the specified AP index number.
status	Shows access points sorted by following status: <ul style="list-style-type: none"> ■ down ■ up
switch <switch-ip-addr>	Shows access points registered with a specified managed device.
unprovisioned	Shows only unprovisioned access points.
usb	Shows USB related parameters.

Examples

The following example shows the information of the APs in the group **default**. The output also includes a description of the flag types that may appear in the **Flags** column.


```

(host) [mynode] #show ap database group default

AP Database
-----
Name      Group      AP Type  IP Address      Status      Flags
Switch IP      Standby IP
-----
ap-205    default    205      191.191.191.252 Up 10d:8h:8m:6s 2p
192.192.189.1 0.0.0.0
ap-215    default    215      191.191.191.253 Up 33d:14h:1m:37s
192.192.189.1 0.0.0.0

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- =
802.1x use factory cert; 2 = Using IKE version 2
4 = WiFi Uplink
B = Built-in AP; C = Cellular RAP; D = Dirty or no config
E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
M = Mesh node
N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires
Auth;
S = Standby-mode AP; T = Thermal ShutDown; U = Unprovisioned; X =
Maintenance Mode
Y = Mesh Recovery
b = bypass of AP1x timeout
c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z =
Datazone AP
p = In deep-sleep status
r = Power Restricted; t = Temperature Restricted

Total APs:2

```

Related Commands

Command	Description
database synchronize	This command configures the Mobility Conductor to synchronize the database with a standby or backup Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.11.0.0	All available flags were included in the flags <flags> sub-parameter.

Release	Modification
ArubaOS 8.8.0.0	A new flag, b , was introduced to show AP1x timeout.
ArubaOS 8.7.0.0	Two new flags, t and r were introduced to indicate Temperature Restriction and Power Restriction respectively.
ArubaOS 8.5.0.0	A new flag, 4 was introduced to indicate Wi-Fi uplink.
ArubaOS 8.4.0.0	A new flag, p was introduced to show that the AP is in deep-sleep mode.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap database-summary

show ap database-summary

Description

Show a general summary of access point information for this controller.

Use this command to show the current number of active APs and Air Monitors. This command is also useful for determining how many unprovisioned APs or duplicate APs are on the network. For full details on each AP registered to a controller, use the command show ap database.

Examples

The output of this command shows that this controller can detect a total of five APs, four up, and one down.

AP Database Summary

```
-----
AP Mode           Total Up  Total Down  Total Upgrading*  Total
Rebooting*  RAP Up  RAP Down  RAP Upgrading*  RAP Rebooting*
-----
- - - - -
Access Points    4        1        0                0
 0      0      0        0                0
Air Monitors     0        0        0                0
 0      0      0        0                0
Wired Access Points 0        0        0                0
 0      0      0        0                0
Mesh Portals     0        0        0                0
 0      0      0        0                0
Mesh Points      0        0        0                0
 0      0      0        0                0
Spectrum Monitors 1        1        0                0
 0      0      0        0                0

*Upgrading and Rebooting counts only reflect APs registered on this controller.
```

The output of this command includes the following information:

Parameter	Description
Total Up	Total number of APs with an <i>up</i> status.
Total Down	Total number of APs with a <i>down</i> status.
IPSEC Up	Total number of APs with an active (up) IPsec tunnel.
IPSEC Down	Total number of APs with an inactive (down) IPsec tunnel.

Related Commands

Command	Description
database-synchronize	This command synchronizes the Mobility Conductor database with a standby or backup Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

```
llad-radio-bond-stats
acl-table
aid-table
airmatch
airmatch-report
anyspot-stats
backup-vap
bandwidth-management
ble-action-status
ble-config
ble-counters
ble-input-filter-stats
ble-log
ble-table
ble-update-status
bss-config
  bss-stats
bucketmap-state
client-deauth-reason-counters
client-info
client-kickout-logs
client-mgmt-counters
client-stats
client-table
client-trace
client-trace clients
cluster-counters
config-msg-history
counters
crash-info
crypto
datapath
dot11r efficiency
dot11r state
  driver-log
esl-status
gre-tun-stats
gsm-counters
hotspot statistics bssid
iot-sniffer
ipc forwarding-statistics
power-table
radio-stats
```

Description

This command displays the AP debugging information. Click parameter links to view the corresponding show commands.

Parameter	Description
<u>11ad-radio-bond-stats</u>	Shows the aggregate 11ad radio bond debug statistics of an AP.
<u>acl-table</u>	Shows ACL table in AP datapath.
<u>aid-table</u>	Shows the association ID table.
<u>airmatch</u>	Shows information about AirMatch.
<u>airmatch-report</u>	Shows information about AirMatch updates on an AP.
<u>anyspot-stats</u>	Shows anyspot statistics of a radio on an AP.
<u>backup-vap</u>	Shows backup VAP for an AP.
<u>bandwidth-management</u>	Shows bandwidth management information for clients.
<u>ble-action-action-status</u>	Shows the action status for BLE devices seen by the AP.
<u>ble-config</u>	Shows the Bluetooth Low Energy (BLE) configuration of the AP.
<u>ble-counter</u>	Shows the packet counters for BLE devices seen by the AP.
<u>ble-input-filter-stats</u>	Shows the input-filter information in the BLE table.
<u>ble-log</u>	Shows the BLE debug logs of the AP.
<u>ble-table</u>	Shows the statistics for BLE devices seen by the AP.
<u>ble-update-status</u>	Shows the configuration update status for BLE devices seen by the AP.
<u>bss-config</u>	Shows the configuration for each BSSID of an AP.
<u>bss-stats</u>	Shows debug and troubleshooting statistics from a specific BSSID of an AP.
<u>bucketmap-state</u>	Shows clients in different buckets.
<u>client-death-reason-counters</u>	Shows the aggregate client death reason counters.
<u>client-info</u>	Shows all the details of a specific client in WLAN driver.
<u>client-kickout-logs</u>	Shows the reasons why clients got deauthenticated due to consecutive TX failures.
<u>client-mgmt-counters</u>	Shows the message counters.
<u>client-stats</u>	Shows the detailed statistics about a client from an AP.

Parameter	Description
<u>client-table</u>	Shows clients associated with an AP.
<u>client-trace</u>	Shows the counts of different types of management data frames traced from a client MAC address.
<u>client-trace clients</u>	Shows debug client trace for all registered clients in an AP.
<u>cluster-counters</u>	Shows the controller cluster statistics.
<u>config-msg-history</u>	Shows recent configuration messages sent and received by an AP.
<u>counters</u>	Shows AP reboot/bootstrap counters.
<u>crash-info</u>	Shows crash log information for an individual AP.
<u>crypto</u>	Shows the debug crypto logs for an AP.
<u>datapath</u>	Shows datapath tunnel parameters of an AP or AP group.
<u>dot11r efficiency</u>	Shows all the r1 keys that are stored in an AP and the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming.
<u>dot11r state</u>	Shows all the r1 keys that are stored in an AP.
<u>driver-log</u>	Shows an AP's driver logs.
<u>esl-status</u>	Shows the ESL status of an AP.
<u>gre-tun-stats</u>	Shows GRE tunnel packet statistics of an AP.
<u>gsm-counters</u>	Shows the GSM counters of an AP or AP group.
<u>hotspot statistics</u>	Shows statistics of ANQP/H2QP information for the specified BSSID.
<u>iot-sniffer</u>	Shows sniffer information on the AP.
<u>ipc forwarding-statistics</u>	Shows an AP's ipc forwarding statistics.
<u>power-table</u>	Shows an AP's Power limit table.
<u>radio-stats</u>	Shows AP's aggregate radio debug statistics.

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>iot-sniffer</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on managed devices.

show ap debug 11ad-radio-bond-stats

```
show ap debug 11ad-radio-bond-stats  
  ap-name <ap-name> | ip-addr <ip-addr>] ip6-addr <ip6-addr>
```

Description

This command displays the aggregate 11ad radio bond debug statistics of an AP.

Parameter	Description
ap-name <ap-name>	Show debugging information for a specific AP.
ip-addr <ip-addr>	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug acl-table

```
show ap debug acl-table {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
```

Description

This command shows ACL table in AP datapath.

Parameter	Description
ap-name <ap-name>	Shows ACL table in AP datapath of an AP specified by AP name.
ip-addr <ip-addr>	Shows ACL table in AP datapath of an AP specified by IP address.
ip6-addr <ip6-addr>	Shows ACL table in AP datapath of an AP specified by IPv6 address.

Example

The following example shows ACL table in AP datapath for an AP named ap-205:

```
(host) [mynode] #show ap debug acl-table ap-name ap-205

acl_2700: entries 21@7680, role, ACL 2700:, acl_flags:0000
0: any any 6 0-65535 80-80 f0000000000080001
1: any any 6 0-65535 135-135 f0000000000080001
2: any any 6 0-65535 445-445 f0000000000080001
3: any any 17 0-65535 67-68 f0000000000080001
4: any any 17 0-65535 53-53 f0000000000080001
5: any any 17 0-65535 123-123 f0000000000080001
6: any any 6 0-65535 23-23 f0000000000080001
7: any any 17 0-65535 69-69 f0000000000080001
8: any any 1 0-65535 2048-2048 f0000000000080001
9: any any 1 0-65535 0-65535 f0000000000080001
10: any any 17 8211-8211 8211-8211 f0000000000080001 hits 41037
11: any any 17 8209-8209 8209-8209 f0000000000080001
12: any any 17 0-65535 514-514 f0000000000080001
13: any any 0 0-65535 0-65535 f0000000000080001
14: user any 17 0-65535 500-500 f0000000000080001
15: any user 17 500-500 500-500 f0000000000080001
16: user any 17 0-65535 4500-4500 f0000000000080001
17: any user 17 4500-4500 4500-4532 f0000000000080001
18: user any 17 0-65535 53-53 f0000000000080001
19: user any 17 53-53 53-85 f0000000000080001
20: any any 0 0-0 0-0 f0000000000180000
acl_2701: entries 1@7700, role, ACL 2701:, acl_flags:0000
0: any any 0 0-0 0-0 f0000000000180000
```

```

acl_2702: entries 2@7701, role, ACL 2702:, acl_flags:0000
0: any 192.168.11.0 255.255.255.0 0 0-0 0-0 f0000000000180001
1: any any 0 0-65535 0-65535 f0000000000180050 po0
acl_2703: entries 1@7703, role, ACL 2703:, acl_flags:0000
0: any any 0 0-0 0-0 f0000000000180001
acl_2704: entries 5@7704, role, ACL 2704:, acl_flags:0000
0: any any 0 0-0 0-0 f0000000000000000
1: any any 0 0-0 0-0 f0000000000180011 po0

```

Related Commands

Command	Description
ip access-list session	This command configures an ACL session. To create IPv6 specific rules, use the ipv6 keyword.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug aid-table

show ap debug aid-table bssid <bssid> [advanced]

Description

This command shows the association ID table.

Parameter	Description
bssid <bssid> [advanced]	Shows association ID table of the specified BSSID.

Example

The following example shows association ID table for the BSSID 00:1a:1e:aa:bb:cc:

```
(host) [mynode] #show ap debug aid-table bssid 00:1a:1e:aa:bb:cc [advanced]
AP Association-ID Table for BSSID: d8:c7:c8:38:fc:f5
-----
AID  MAC
---  ---
1    80:86:f2:41:1f:1d
2    80:86:f2:41:1e:f0
3    80:86:f2:41:1e:be

Total AID count: 3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug airmatch

```
show ap debug airmatch channel-lists | feasibility | nbr | reporting-radio | status  
  {[ap-name <ap-name>]}|[ip-addr <ip-addr>]}|[ip6-addr <ip6-addr>]}
```

Description

This command displays information about AirMatch.

Parameter	Description
channel-lists	Shows channel lists.
feasibility	Shows radio feasibility data.
nbr	Shows the list of neighboring radios.
reporting-radio	Shows the reporting radio details.
status	Shows the status of the radios.
ap-name <ap-name>	Shows AirMatch data on an AP specified by AP name.
ip-addr <ip-addr>	Shows AirMatch data on an AP specified by IP address.
ip6-addr <ip6-addr>	Shows AirMatch data on an AP specified by IPv6 address.

Example

The following example shows information about AirMatch reporting radio of an AP that is identified by its name.

```
(host) #show ap debug airmatch reporting-radio ap-name x4  
  
AirMatch Reporting Radio Band 5GHz  
-----  
Item                               Value  
----                               -  
Required                           Yes  
Eth Mac                             18:64:72:cf:e3:cc  
Radio Mac                           18:64:72:7e:3c:d0  
AP Name                             x4  
AP Model                             AP-335  
Radio Number                         0  
Band                                 5GHz  
Channel                             36  
Bandwidth (MHz)                     40  
Channel Reason                       AirMatch - Solver  
EIRP (dBm)                          15.0
```

```

EIRP Reason          AirMatch - Solver
Active               Yes
Static Chan         No
Static EIRP         No
Time Zone           PST8PDT,M3.2.0,M11.1.0
Deploy Hour         N/A
AP Deploy Hour      N/A
Advance Power Control Yes
Probe Type          sap
Time Zone (Olson)   America/Los_Angeles
Radio number        0
Radio Client Preference Allow All Solver Assigned
Band Preference     Full

```

AirMatch Reporting Radio Band 2.4GHz

```

-----
Item                 Value
-----
Required             Yes
Eth Mac              18:64:72:cf:e3:cc
Radio Mac            18:64:72:7e:3c:c0
AP Name              x4
AP Model             AP-335
Radio Number         1
Band                 2.4GHz
Channel              N/A
Bandwidth (MHz)     N/A
Channel Reason       AirMatch - Solver
EIRP (dBm)          N/A
EIRP Reason          AirMatch - Solver
Active               Yes
Static Chan         No
Static EIRP         No
Time Zone           PST8PDT,M3.2.0,M11.1.0
Deploy Hour         N/A
AP Deploy Hour      N/A
Advance Power Control Yes
Probe Type          airmatch-am
Time Zone (Olson)   America/Los_Angeles
Radio number        1
Radio Client Preference Allow All Solver Assigned
Band Preference     Full

```

The following example shows information about AirMatch channel list.

```

(host) #show ap debug airmatch channel-lists ap-name AP_205
Radio 0 Configuration
-----
Key                 Value
-----
Probe Type          sap
Scan Mode           all-reg-domain
Dual 5GHz Mode      Disabled
Flex Radio Mode     2.4GHz-and-5GHz

```

Split-5GHz Mode Disabled
Num of Supported Opmodes 0
Radio 0 Ext Cfg

Band 5GHz

CSR Threshold 0
Deploy Hour 255
EIRP Max 21
EIRP Min 15
EIRP Offset 0
Max Channel BW 80MHz
Min Channel BW 20MHz
Mode sap
Radio Enabled
HE Mode Enabled
HT Mode Enabled
VHT Mode Enabled

Radio 0 Channel List

Channel	Default	Flags
-----	-----	-----
34	-	DYp
36	Y	DVACLYFETSp
38	-	DYp
40	Y	DVACUYBPTSp
42	-	DYp
44	Y	DVACLYFBTSp
46	-	DYp
48	Y	DVACUYBPTSp
52	Y	DVACLYFETXSp
56	Y	DVACUYBPTXSp
60	Y	DVACLYFBTXSp
64	Y	DVACUYBPTXSp
100	-	DACLYp
104	-	DACUYp
108	-	DACLYp
112	-	DACUYp
116	-	DACLYp
120	-	DACUYp
124	-	DACLYp
128	-	DACUYp
132	-	DACLYp
136	-	DACUYp
140	-	DACLYp
144	-	DACUYp
149	Y	DVACLYFETSp
153	Y	DVACUYBPTSp
157	Y	DVACLYFBTSp
161	Y	DVACUYBPTSp
165	Y	DVACTSp
169	-	DCp
173	-	DCp

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Pre

```

sent, Y: Scan 80MHz,
L: Scan Secondary Above, U: Scan Secondary Below, Z: Rare Channel
V: Valid, T: Valid 20MHz Channel, F: Valid 40MHz Channel, P: Val

Channel Pair
E: Valid 80/80+80MHz Channel (First 20M), B: Belongs to valid 80/

channel
G: Valid 160MHz Channel (First 20M), Q: Belongs to valid 160MHz c

O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N: Split

Scan
R: Radar detected in last 30 min, X: DFS required, S: Transmit Al

J: Unconventional Scan 40MHz Above, M: Unconventional Scan 40MHz

b: Out-of-band scan Channel (valid only for dual 5GHz mode), p: P

Preference
q: Zero Wait DFS

```

The following example shows information about AirMatch status.

```

(host) #show show ap debug airmatch status ap-name ap635
AirMatch Reporting Radio Band 5GHz
-----
Variable                               State
-----
Solver Channel                          N/A
Static Channel                          149E
Periodic Check Backoff Time(secs)      22
Invalid Bandwidth                       0
Invalid EIRP                            0
Reg Domain                              0
Invalid DRT                             0
Clean Sate                              0
Radio Client Preferecne                 0
Config Min CBW change                   0
Config Max CBW change                   0
Min Channel BW Limitation                0
Solver Channel Info
-----
Blocked Reason   Time left
-----
Radar           0

```


High Noise 0
Number of Radar and Noise Events in the last 24hrs

```
-----  
Channel  High Noise  Radar  
-----  
36      0           0  
40      0           0  
44      0           0  
48      0           0  
100     0           0  
104     0           0  
108     0           0  
112     0           0  
149     0           0  
153     0           0  
157     0           0  
161     0           0  
165     0           0
```

AirMatch Reporting Radio Band 2.4GHz

```
-----  
Variable                               State  
-----  
Solver Channel                         N/A  
Static Channel                         6  
Periodic Check Backoff Time(secs)     22  
Invalid Bandwidth                      0  
Invalid EIRP                           0  
Reg Domain                             0  
Invalid DRT                            0  
Clean Sate                             0  
Radio Client Preferecne                0  
Config Min CBW change                  0  
Config Max CBW change                  0  
Min Channel BW Limitation              0  
Solver Channel Info
```

```
-----  
Blocked Reason  Time left  
-----  
High Noise 0  
Noise events in last 24hrs
```

```
-----  
Channel  High Noise  
-----  
1      0  
5      0  
6      0  
7      0  
11     0
```

AirMatch Reporting Radio Band 6GHz

```
-----  
Variable                               State  
-----  
Solver Channel                         N/A  
Static Channel                         101S
```

Periodic Check Backoff Time(secs) 0
Invalid Bandwidth 0
Invalid EIRP 0
Reg Domain 0
Invalid DRT 0
Clean Sate 0
Radio Client Preferecne 0
Config Min CBW change 0
Config Max CBW change 0
Min Channel BW Limitation 0
Solver Channel Info

Blocked Reason Time left

High Noise 0
Noise events in last 24hrs

Channel High Noise

21 0
25 0
29 0
33 0
37 0
41 0
45 0
49 0
53 0
57 0
61 0
65 0
69 0
73 0
77 0
81 0
85 0
89 0
93 0
97 0
101 0
105 0
109 0
113 0
117 0
121 0
125 0
129 0
133 0
137 0
141 0
145 0
149 0
153 0
157 0
161 0
165 0

```
169      0
173      0
```

The following example shows information about AirMatch channel list on AP-635 access point (Wi-Fi 6E AP).

```
(Aruba7240XM_04_5A_48) #show ap debug airmatch channel-lists ap-name ap635-1-om
```

```
Radio 0 Configuration
```

```
-----
Key                               Value
---                               -
Probe Type                        sap
Scan Mode                         all-reg-domain
Dual 5GHz Mode                    Enabled
Flex Radio Mode                   2.4GHz-and-5GHz
Split-5GHz Mode                   Enabled
Num of Supported Opmodes          0
```

```
Radio 0 Ext Cfg
```

```
-----
Band                               5GHz
----                               -
CSR Threshold                      0
Deploy Hour                        255
EIRP Max                           21
EIRP Min                           15
EIRP Offset                         0
Max Channel BW                     80MHz
Min Channel BW                     20MHz
Mode                                sap
Radio                              Enabled
HE Mode                            Enabled
HT Mode                            Enabled
VHT Mode                           Enabled
```

```
Radio 0 Channel List
```

```
-----
Channel  Default  Flags
-----  -
34       -          DY
36       Y          DVACLYFETS
38       -          DY
40       Y          DVACUYBPTSJ
42       -          DY
44       Y          DVACLYFBTSM
46       -          DY
48       Y          DVACUYBPTSJ
52       -          DACLYXSM
56       -          DACUYXSJ
60       -          DACLYXSM
64       -          DACUYXS
```

```

100      -      DACLYXS
104      -      DACUYXSJ
108      -      DACLYXSM
112      -      DACUYXSJ
116      -      DACLYXSM
120      -      DACUYXSJ
124      -      DACLYXSM
128      -      DACUYXSJ
132      -      DACLYXSM
136      -      DACUYXSJ
140      -      DACLYXSM
144      -      DCUYXS
149      Y      DVACLYFETS
153      Y      DVACUYBPTSJ
157      Y      DVCLYFBTSM
161      Y      DVCUYBPTS
165      Y      DVACTS
169      -      D
173      -      D

```

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present, Y: Scan 80MHz,

L: Scan Secondary Above, U: Scan Secondary Below, Z: Rare

Channel

V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel, P:

Valid 40MHZ Channel Pair

E: Valid 80/80+80MHz Channel (First 20M), B: Belongs to valid

80/80+80MHz channel

G: Valid 160MHz Channel (First 20M), Q: Belongs to valid

160MHz channel

O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N:

Split Channel Scan

R: Radar detected in last 30 min, X: DFS required, S:

Transmit Allowed

J: Unconventional Scan 40MHz Above, M: Unconventional Scan

40MHz Below

b: Out-of-band scan Channel (valid only for dual 5GHz mode),

p: Pooling Preference

q: Zero Wait DFS u: UTB filtered channel, W: Scan 160MHz,

Radio 1 Configuration

```

Key                Value
---                -
Probe Type         sap
Scan Mode          all-reg-domain
Dual 5GHz Mode     Enabled
Flex Radio Mode    2.4GHz-and-5GHz
Split-5GHz Mode    Enabled
Num of Supported Opmodes 0

```

Radio 1 Ext Cfg

```

Band              2.4GHz
-----

```

```

CSR Threshold      0
Deploy Hour       255
EIRP Max          12
EIRP Min          6
EIRP Offset       0
Max Channel BW    20MHz
Min Channel BW    20MHz
Mode              sap
Radio             Enabled
HE Mode          Enabled
HT Mode          Enabled
VHT Mode         Disabled

```

Radio 1 Channel List

```

-----
Channel  Default  Flags
-----  -
1        Y        DVCLFTSp
2        -        DCLSp
3        -        DACLSp
4        -        DACLSp
5        Y        DVCULPSp
6        Y        DVACULTSp
7        Y        DVACULFSp
8        -        DCULSp
9        -        DCULSp
10       -        DACUSp
11       Y        DVACUPTSp
12       -        DUUp
13       -        DUUp
14       -        Dp

```

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present, Y: Scan 80MHz,

L: Scan Secondary Above, U: Scan Secondary Below, Z: Rare

Channel

V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHZ Channel, P:

Valid 40MHZ Channel Pair

E: Valid 80/80+80MHZ Channel (First 20M), B: Belongs to valid

80/80+80MHZ channel

G: Valid 160MHZ Channel (First 20M), Q: Belongs to valid

160MHZ channel

O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N:

Split Channel Scan

R: Radar detected in last 30 min, X: DFS required, S:

Transmit Allowed

J: Unconventional Scan 40MHz Above, M: Unconventional Scan

40MHz Below

b: Out-of-band scan Channel (valid only for dual 5GHz mode),

p: Pooling Preference

q: Zero Wait DFS u: UTB filtered channel, W: Scan 160MHz,

Radio 2 Configuration

```

-----
Key          Value

```

```

---
Probe Type                sap
Scan Mode                 all-reg-domain
Dual 5GHz Mode           Enabled
Flex Radio Mode          2.4GHz-and-5GHz
Split-5GHz Mode         Enabled
Num of Supported Opmodes 0

```

Radio 2 Ext Cfg

```

-----
Band                6GHz
-----
CSR Threshold       0
Deploy Hour        255
EIRP Max           127
EIRP Min           1
EIRP Offset        0
Max Channel BW     160MHz
Min Channel BW     80MHz
Mode               sap
Radio              Enabled
HE Mode            Enabled
HT Mode            Enabled
VHT Mode           Enabled

```

Radio 2 Channel List

```

-----
Channel  Default  Flags
-----
1        -        DCLYWpu
5        -        DCUYWJpxu
9        -        DCLYWpu
13       -        DCUYWJpu
17       -        DCLYWpu
21       -        DACUYWJpxu
25       -        DCLYWpu
29       Y        DVCUYWTSJp
33       Y        DVCLYWFEGETSp
37       Y        DVACUYWBQPTSJpx
41       Y        DVCLYWFBQTSp
45       Y        DVCUYWBQPTSJp
49       Y        DVCLYWFEQTSp
53       Y        DVACUYWBQPTSJpx
57       Y        DVCLYWFBQTSp
61       Y        DVCUYWBQPTSJp
65       Y        DVCLYWFEGETSp
69       Y        DVACUYWBQPTSJpx
73       Y        DVCLYWFBQTSp
77       Y        DVCUYWBQPTSJp
81       Y        DVCLYWFEQTSp
85       Y        DVACUYWBQPTSpx
89       Y        DVCYWFBQTSp
93       Y        DVCYWBQPTSJp
97       Y        DVCLYWFEGETSp

```

```

101      Y      DVACUYWBQPTSJpx
105      Y      DVCLYWFBQTSp
109      Y      DVCUYWBQPTSJp
113      Y      DVCLYWFEQTSp
117      Y      DVCUYWBQPTSJpx
121      Y      DVCLYWFBQTSp
125      Y      DVCUYWBQPTSJp
129      Y      DVCLYWFEQTSp
133      Y      DVCUYWBQPTSJpx
137      Y      DVCLYWFBQTSp
141      Y      DVCUYWBQPTSJp
145      Y      DVCLYWFEQTSp
149      Y      DVCUYWBQPTSJpx
153      Y      DVCLYWFBQTSp
157      Y      DVCUYWBQPTSJp
161      Y      DVCLYWFEQTSp
165      Y      DVACUYWBQPTSJpx
169      Y      DVCLYWFBQTSp
173      Y      DVCUYWBQPTSJp
177      Y      DVCLYWFEQTSp
181      Y      DVCUYWBQPTSJpx
185      Y      DVCLYWFBQTSp
189      Y      DVCUYWBQPTSJp
193      Y      DVCLYWFEQTSp
197      Y      DVACUYWBQPTSJpx
201      Y      DVCLYWFBQTSp
205      Y      DVCUYWBQPTSJp
209      Y      DVCLYWFEQTSp
213      Y      DVACUYWBQPTSJpx
217      Y      DVCLYWFBQTSp
221      Y      DVCUYWBQPTSJp
225      Y      DVCLYWFTSp
229      Y      DVCUYWPTSpx
233      -      DCYWp

```

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present, Y: Scan 80MHz,

L: Scan Secondary Above, U: Scan Secondary Below, Z: Rare Channel

V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHZ Channel, P: Valid 40MHZ Channel Pair

E: Valid 80/80+80MHz Channel (First 20M), B: Belongs to valid 80/80+80MHz channel

G: Valid 160MHz Channel (First 20M), Q: Belongs to valid 160MHz channel

O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N: Split Channel Scan

R: Radar detected in last 30 min, X: DFS required, S: Transmit Allowed

J: Unconventional Scan 40MHz Above, M: Unconventional Scan 40MHz Below

b: Out-of-band scan Channel (valid only for dual 5GHz mode), p: Pooling Preference

q: Zero Wait DFS u: UTB filtered channel, W: Scan 160MHz,

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.10.0.0	The output of the command was modified to include the <code>Probe Type</code> parameter under the AirMatch Reporting Radio Band 2.4GHz table.
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The Radio 2 interface was displayed for 6 GHz band on Wi-Fi 6E APs. ■ The command output was modified to include 6 GHz values for Wi-Fi 6E APs. ■ The <code>show ap debug airmatch channel-lists ap-name <ap-name></code> command output was modified to include <code>u</code> channel flag and 6 GHz data for Wi-Fi 6E APs. ■ All instances of <code>Blacklist Reason</code> have been replaced with <code>Blocked Reason</code>.
ArubaOS 8.6.0.0	A new interface for Radio 2 will be displayed for AP-555 access points.
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug airmatch-report

```
show ap debug airmatch-report {[ap-name <ap-name>]}|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]
```

Description

This command displays information about AirMatch updates on an AP. Issue this command to show AirMatch measurement settings applied to the selected AP, as well as information about the last update for different AirMatch reports.

Parameter	Description
ap-name <ap-name>	Shows AirMatch data on an AP specified by AP name.
ip-addr <ip-addr>	Shows AirMatch data on an AP specified by IP address.
ip6-addr <ip6-addr>	Shows AirMatch data on an AP specified by IPv6 address.

Example

The following example shows the latest AirMatch statistics on the AP **Floor2-west**.

```
(Host) [node] #show ap debug airmatch-report ap-name Floor2-west

AirMatch measure info
-----
report period (mins)  measure duration (mins)  measure state  report enabled
-----
5                    5                        in progress   yes
AirMatch report info
-----
AirMatch Report Type  Count  Last Update Time
-----
reporting radio       2      2016-07-05 22:01:12
neighbors             8000   2016-07-06 22:46:09
feasibility           730    2016-07-06 22:47:44
event                 0      no update
```

The output of this command includes the following information:

Column	Description
report period	The AirMatch report period in the ap system profile
measure duration	The AirMatch measure duration in the ap system profile

Column	Description
<code>measure state</code>	The current AirMatch measurement state. Possible states are in progress , stopped , and waiting .
<code>Report enabled</code>	This value is expected to be the same as the airmatch-report-enabled setting in the ap system profile.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the <code>airmatch ap freeze</code> command uses a static radio configuration until those settings get explicitly canceled with the <code>airmatch ap unfreeze</code> command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug anyspot-stats

```
show ap debug anyspot-stats {[ap-name <ap-name>]} [[ip-addr <ip-addr>]] [[ip6-addr <ip6-addr>]] {radio <radio>}
```

Description

This command shows anyspot statistics of a radio on an AP.

Parameter	Description
ap-name <ap-name>	Shows anyspot statistics of a radio on an AP specified by AP name.
ip-addr <ip-addr>	Shows anyspot statistics of a radio on an AP specified by IP address.
ip6-addr <ip6-addr>	Shows anyspot statistics of a radio on an AP specified by IPv6 address.
radio <radio>	Shows ACL table in AP datapath of AP specified by radio ID (either 0,1 or 2).

Example

The following example shows anyspot is disabled on radio 0 of an AP named ap-205:

```
(host) [mynode] #show ap debug anyspot-stats ap-name ap-205 radio 0
Anyspot is disabled on the specified radio!
```

Related Commands

Command	Description
wlan anyspot-profile	The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.

Command History

Release	Modification
ArubaOS 8.6.0.0	Radio ID 2 was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug backup-vap

```
show ap debug backup-vap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]}
```

Description

This command shows backup VAP for an AP.

Parameter	Description
ap-name <ap-name>	Shows backup VAP for an AP for specified AP name.
ip-addr <ip-addr>	Shows backup VAP for an AP for specified IP address.
ip6-addr <ip6-addr>	Shows backup VAP for an AP for specified IPV6 address.

Example

The following example shows backup VAP for an AP named ap-205:

```
(host) [mynode] #show ap debug backup-vap ap-name ap-205

AP backup ssid debug information
-----
Item      Value
-----
Host      192.192.189.1
Config    Mode:off  Band:all
Run:      Telnet[N] Enable[0] aruba015[N] aruba115[N]
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug bandwidth-management

```
show ap debug bandwidth-management [ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
```

Description

This command shows bandwidth management information for clients.

Parameter	Description
ap-name <ap-name>	Name of the access point.
ip-addr <ip-addr>	IP address of the access point.
ip6-addr <ip6-addr>	IPv6 address of the access point

Examples

The output of this command shows interface and shaping and interface policy for this AP.

```
(host) #show ap debug bandwidth-management ap-name amit-ap-105
Interface :wifi0
Shaping policy:Default-access (no stats)
Interface :wifi1
Shaping policy:Default-access (no stats)
```

Related Commands

Command	Description
aaa bandwidth-contract	This command configures a bandwidth contract.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-action-status

```
show ap debug ble-action-status {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the action status for BLE devices seen by the AP.

Syntax

Parameter	Description
ap-name	Displays the action status for BLE devices seen by the AP based on the AP name.
ip-addr	Displays the action status for BLE devices seen by the AP based on the IPv4 address.
ip6-addr	Displays the action status for BLE devices seen by the AP based on the IPv6 address.

Example

The output of this command displays the action status for BLE devices seen by the AP.

```
(host) #show ap debug ble-action-status ap-name ap325

BLE Device Action Table
-----

Pending Actions
-----
BLE Device MAC  ActionId  Operation  Characteristic  Value  Status
-----

Completed Actions
-----
BLE Device MAC  ActionId  Operation  Characteristic  Value  Status
-----
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-config

```
show ap debug ble-config
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the Bluetooth Low Energy (BLE) configuration of the AP. In addition, the command displays the update interval to the Beacon Management Console (BMC), BLE token, AP Beacon (APB) status, the last update time to BMC, and the beacon MAC for which the last update was sent.



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Parameter	Description
ap-name	Displays the BLE configuration of an AP for a specific AP based on the AP name.
ip-addr	Displays the BLE configuration of an AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the BLE configuration of an AP for a specific AP based on the IPv6 address.

Example

The output of this command displays the update interval to the Beacon Management Console (BMC), BLE token, AP Beacon (APB) status, the last update time to BMC, and the beacon MAC for which the last update was sent.

```
(host) #show ap debug ble-config ap-name ap325
BLE Configuration
-----
Item                               Value
----                               -
LMS IP                              192.0.2.1
Authorization Token
YzJlNmEzOTMtYjE4MC00ZTc4LWJmNDEtMzMzNGEYyY2NjY2RmOj
Y4YzBhOWI2LWYxMGQtNGZlMi05YmVkLTI5ZTY5MDNkYjhmYQ==
Endpoint URL
https://edit.meridianapps.com/api/beacons/manage
BLE Ready                            Yes
Update Intvl (in sec)                300
BLE debug log                         Enabled
```

```

Operational Mode          Beaconing (APB: Beaconing)
Uplink Status            Up (APB: -NA-)
APB Connection Status    0
Last BLE Device Update Attempt c4:be:84:19:ef:99
Last Update Sent Time    2015-09-27 11:45:50
-----

```

Notes: - Setting Message Selector value to 0x0 will cause the APB to function improperly. Use the knob with caution.

- An active Meridian Beacons Management profile will override the iBeacon configuration setting on an AP's BLE radio.
- Uplink status is applicable only when console is set to dynamic

For APBs of type LS-BT1USB, applied operational mode is Beaconing if ap system profile setting is either Persistent or Dynamic.

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-counters

```
show ap debug ble-counters
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the packet counters for BLE devices seen by the AP. In addition, the command displays if any high power beacons are seen, the time at which configuration update was received for the beacons from the BMC and the updated response sent back.



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Parameter	Description
ap-name	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the AP name.
ip-addr	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the IPv6 address.

Example

The output of this command displays the packet counters for BLE devices seen by the AP. In addition, it displays if any high power beacons are seen, the time at which configuration update was received for the beacons from the BMC and the updated response sent back.

```
(host) #show ap debug ble-counters ap-name ap325

BLE Device Table
-----
MAC          RSSI          Major#  Minor#  iBeacon  ScanRspV0  ScanRspV1  HiPwr
-----
d0:39:72:d5:43:75  1000  1215  453  0  62
  4 -71
c4:be:84:19:8b:a3  0  0  617  0  6
  4 -81
c4:be:84:19:ec:67  0  0  604  0  1
  4 -83
```

```

d0:39:72:d4:fa:9c 6      1      1      0      0
0 -89
c4:be:84:19:ef:99 1000   1374   126    0      0
0 --
78:a5:04:15:23:35 1000   1222   445    0      47
1 -70
c4:be:84:19:ec:2f 0      0      575    0      1
5 -84

LastUpdate  CfgRx    CfgTx
-----
4s          NoUpdate NoUpdate
4s          NoUpdate NoUpdate
4s          NoUpdate NoUpdate
1292s      NoUpdate NoUpdate
4s          NoUpdate NoUpdate
4s          NoUpdate NoUpdate
4s          NoUpdate NoUpdate

Total beacons:7
Total serial bytes read from APB:138761
Total msg bytes processed:138761
Total serial bytes dropped:0

```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-input-filter-stats

```
show ap debug ble-input-filter-stats
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the input-filter information in the BLE table.

Parameter	Description
ap-name	Displays the input-filter information in the BLE table for a specific AP based on the AP name.
ip-addr	Displays the input-filter information in the BLE table for a specific AP based on the IPv4 address.
ip6-addr	Displays the input-filter information in the BLE table for a specific AP based on the IPv6 address.

Example

The output of this command displays input-filter information in the BLE table.

```
(host) [mynode] #show ap ble-input-filter-stats ap-name ap325

BLE Table Input Filter Stats
-----
Input Filtering: Enabled

Filtered Devices
-----
MAC Address          Last Updated
-----
98:7b:f3:49:a8:79    0s
50:65:83:a4:b6:cf    0s
88:c2:55:d1:f6:d3    0s
f8:60:65:44:f2:11    0s
20:4c:03:7f:4a:94    0s
f9:61:66:45:f3:12    0s
20:4c:03:44:24:a3    0s
20:4c:03:39:e6:dd    0s
54:6c:0e:2a:18:60    0s
50:f1:4a:f5:c3:f7    0s
b8:27:eb:a1:a0:c0    0s
88:c2:55:d1:c7:67    0s
54:6c:0e:2a:14:83    0s
20:4c:03:a4:a8:9d    0s
```

```
fa:62:67:46:f4:13 0s
50:f1:4a:f5:96:3c 1s
50:31:ad:00:0e:de 1s
54:6c:0e:2a:19:3f 1s
a0:e6:f8:38:05:f8 1s
20:4c:03:45:c4:82 1s
50:31:ad:02:5c:97 2s
fc:64:69:48:f6:15 3s
a0:e6:f8:38:0f:40 3s
60:12:83:de:00:6e 4s
20:4c:03:84:21:b8 8s
50:31:ad:00:62:8f 12s
20:4c:03:84:21:d4 21s
20:4c:03:84:1c:d4 35s
20:4c:03:84:21:f2 38s
20:4c:03:a7:bc:bb 23754s
50:65:83:79:a6:32 23754s
f0:5c:19:c9:ca:8f 23754s
20:4c:03:a7:bc:d4 23754s
38:81:d7:40:54:a4 23754s
f0:5c:19:c9:db:47 23754s
20:4c:03:13:9f:9f 23754s
20:4c:03:bd:c4:cc 23754s
50:65:83:79:52:86 23754s
20:4c:03:8e:92:90 23754s
c4:d9:09:b5:b2:34 23754s
20:4c:03:39:e3:54 23754s
20:4c:03:13:8a:dd 23755s
38:81:d7:40:64:0c 23755s
20:4c:03:7d:d3:ca 23755s
38:81:d7:40:64:7d 23755s
20:4c:03:39:e2:a2 23757s
20:4c:03:84:21:fa 23757s
20:4c:03:84:1d:15 23758s
8c:8b:83:3d:d2:d0 23758s
f4:b8:5e:43:47:14 23758s
38:81:d7:40:4d:15 23759s
20:4c:03:13:b8:e6 23759s
20:4c:03:13:9e:22 23759s
50:65:83:79:60:d3 23759s
f4:b8:5e:43:17:6e 23759s
50:65:83:79:5d:ad 23760s
a0:e6:f8:37:0f:f3 23760s
20:4c:03:13:b4:17 23764s
20:4c:03:84:1d:41 23792s
8c:8b:83:3e:c4:99 196828s
20:4c:03:84:21:ba 196830s
50:65:83:79:a5:18 196830s
40:bd:32:a8:e7:5c 196837s
50:65:83:79:5d:f3 196902s
```

```
List Size:      64 entries
List Capacity: 64 entries
```

Related Commands

Command	Description
ap ble-init-action	This command enables or disables the input-filter.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-log

```
show ap debug ble-log
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the BLE debug logs of the AP.

Parameter	Description
ap-name	Displays the BLE debug logs of an AP for a specific AP based on the AP name.
ip-addr	Displays the BLE debug logs of an AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the BLE debug logs of an AP for a specific AP based on the IPv6 address.



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Example

The output of this command displays BLE process logs in the AP.

```
(Aruba7220) #show ap debug ble-log ap-name ap325
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest:377 ble_
token:YzJlNmEzOTMtYjE4MC00ZTc4LWJmNDEtMzMzNGEyY2NjY2RmOjY4YzBhOWI2LWYxMGQtNG
ZlMi05YmVklTI5ZTY5MDNkYjhmYQ==. length:100
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest:378 ble_
url:https://edit.meridianapps.com/api/beacons/manage. length:48
[2127]2015-10-27 11:45:50 construct_bmrequest_payload:1265
mac:d0:39:72:d4:fa:9c retry bmreq later... some attr pending (1/1/1/0/0).
[2127]2015-10-27 11:45:50 construct_bmrequest_payload:1337 6/7 beacons added
to JSON. Total beacons processed:7/7
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest: Sending BMRequest msg to
ble_relay@192.0.2.2[100/48] jsonlen:2145
[2127]2015-10-27 11:45:51 ble_ap_handle_bmresponse_msg:222 Result from
172.20.1.1:8505 strlen:30 footer:0xdeadbeef
[2127]2015-10-27 11:45:51 dwas_command:(nil) 1.
[2127]2015-10-27 11:45:51 process_json_response_from_ble_relay:2623 next_
sync[0]:300 dwas_command[0]:(null) updates array size is 0.
```

```

[2127]2015-10-27 11:45:56 msglen=90 :: 04 ff 57 f5 00 06 99 ef 19 84 be c4
0d 01 02 03 01 83 01 02 e8 03 02 02 5e 05 0f 10 09 45 8c 20 45 86 4e d3 8d
2f a0 84 2a cb d6 e6 06 01 02 07 01 08 08 01 01 09 01 01 0a 01 01 0b 01 26
0c 04 20 07 01 00 18 0b db 19 00 00 02 99 ef 19 84 be c4 1a 01 03 19 01 00
04 01 00
[2127]2015-10-27 11:45:56 update_ble_data:2347 cmd status: seq_num: 6619
(19db) app_err (0): Good sys_err: 0 progress (2): Done upg_progress[0]:
0.
[2127]2015-10-27 11:45:58 ageout_ble_device:694 numentries:7 sizeof(ble_mon_
data_t):520.
[2127]2015-10-27 11:46:16 msglen=90 :: 04 ff 57 f5 00 06 99 ef 19 84 be c4
0d 01 02 03 01 83 01 02 e8 03 02 02 5e 05 0f 10 09 45 8c 20 45 86 4e d3 8d
2f a0 84 2a cb d6 e6 06 01 02 07 01 08 08 01 01 09 01 01 0a 01 01 0b 01 26
0c 04 34 07 01 00 18 0b db 19 00 00 02 99 ef 19 84 be c4 1a 01 03 19 01 00
04 01 00
[2127]2015-10-27 11:46:16 update_ble_data:2347 cmd status: seq_num: 6619
(19db) app_err (0): Good sys_err: 0 progress (2): Done upg_progress[0]:
0.

```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-table

```
show ap debug ble-table
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  ibeacon
```

Description

This command displays the statistics for BLE devices seen by the AP. In addition, the command displays beacons seen by the APB, each of the beacons' attributes such as the Major-Minor numbers, Batter Level, Firmware version, time since the beacon was last heard by the APB.



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Parameter	Description
ap-name	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the AP name.
ip-addr	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the IPv6 address.
ibeacon	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the ibeacon info.

Example

The output of this command displays the statistics for BLE devices seen by the AP.

```
(host) #show ap debug ble-table ap-name ap325

BLE Device Table
-----
MAC          HW_Type  FW_Ver      Flags      Status  Batt(%)  RSSI
Major#  Minor#
-----  -----  -----  -----  -----  -----  -----
d0:39:72:d5:43:75  LS-BT1   OAD A 1.1-25  0x0001  IAH      100      -71
1000      1215
c4:be:84:19:8b:a3  LS-BT1USB OAD B 1.1-25  0x0003  IAH      USB      -83      0
0
```

```

c4:be:84:19:ec:67 0 OCTOMORE OAD B 1.1-26 0x0003 IAH -- -74 0
c4:be:84:19:ef:99 1000 1374 OCTOMORE OAD B 1.1-38 0x0083 LIA -- --
78:a5:04:15:23:35 1000 1222 LS-BT1 OAD A 1.1-25 0x0001 IAH 100 -79
c4:be:84:19:ec:2f 0 OCTOMORE OAD B 1.1-26 0x0003 IAH -- -83 0

```

UUID	Tx_Power	Last Update	Uptime
5D3BCC63-BD6B-4FAF-906F-91C91519A69B	13	8s	11h:3m:0s
4152554E-F99B-4A3B-86D0-947070693A78	14	4s	23h:51m:30s
4152554E-F99B-4A3B-86D0-947070693A78	14	0s	19h:38m:30s
09458C20-4586-4ED3-8D2F-A0842ACBD6E6	2	4s	18h:45m:0s
09458C20-4586-4ED3-8D2F-A0842ACBD6E6	13	0s	22h:36m:0s
4152554E-F99B-4A3B-86D0-947070693A78	14	0s	19h:39m:0s

Total beacons:6

APB UI:[0/NO_UPGRADE_REQD]:65535(0xffff) blks:0/0 rep:0 total:0(0x0)

APB UI:upg_b_status-next:0x00/ooo:0x00/next2:0x00/upg_b:0x00/allrx:0x00/oooBlk:0x00/oooBlk:0x00/oooBlk:0x00

APB UI:upg_b_status_errs-inv_upg:0x00/inv_cmd:0x00/inv_op:0x00/buf_tl:0x00/good:0x00

APB UI:acks/ka-From APB:0x00/0x00 From app:0x00,0x00/0x00

APB UI Clock:Start:1969-12-31 16:00:00 End:1969-12-31 16:00:00

Current:2015-10-27 11:48:20

Note: Battery level for LS-BT1USB devices is indicated as USB.

Note: Uptime is shown as Days hour:minute:second.

Note: Last Update is time in seconds since last heard update.

Status Flags:L:AP's local beacon; I:iBeacon; A: Aruba Beacon; H: Aruba HiPower Beacon

:U:Image Upgrade Pending

The output of this command displays the statistics for BLE devices seen by the AP when ibeacon option is used.

```

(VMC-5.239) [mynode] #show ap debug ble-table ap-name AP505h_solum ibeacon
BLE Device Table [iBeacon]

```

MAC	Major	Minor	UUID	Meas.
28:de:65:44:8a:68	--	--	--	--
-79	I:122s			
ac:23:3f:a9:d0:7f	0	0	E2C56DB5-DFFB-48D2-B060-D0F5A71096E0	-59
-24	I:0s			
3c:a3:08:93:53:04	0	0	4152554E-F99B-4A3B-86D0-947070693A78	--
-82	I:269s			
20:4c:03:b2:79:1c	0	0	4152554E-F99B-4A3B-86D0-947070693A78	-56
-91	I:2s			
20:4c:03:44:23:58	--	--	--	--
-90	I:29s			

```

5c:f8:21:e6:d5:58 0 0 4152554E-F99B-4A3B-86D0-947070693A78 -56
-39 I:0s
54:6c:0e:15:7b:5f 0 0 4152554E-F99B-4A3B-86D0-947070693A78 -60
-37 I:0s
54:6c:0e:15:6b:c6 0 0 4152554E-F99B-4A3B-86D0-947070693A78 -60
-36 I:0s

```

Note: Battery level for

LS-BT1USB devices is indicated as USB.

Note: Uptime is shown as Days hour:minute:second.

Note: Last Update is time in seconds since last heard update.

Note: Meas. Pow. is the averaged RSSI (in dBm) when the iBeacon is calibrated.

Note: Tx_Power is shown in dBm in the APBs section for radios that support radio profile type 1. For all other APB radios, Tx_Power is a discrete level from 0-15.

Status Flags:L:AP's local beacon; I:iBeacon; A:Beacon management capable
:H:High power beacon; T:Asset Tag Beacon; U:Upgrade of firmware pending

:u:Beacon management update received

Last Update Flags:I: Device observed by internal radio

:E: Device observed by external radio

Generic Filter:S:serviceUUIDFilter; C:companyIdentifierFilter

:M:macOUIFilter; L:localNameFilter(VMC-5.239) [mynode] #show

ap debug ble-table ap-name AP505h_solum allBLE Device Table [APBs]

```

-----
MAC                HW_Type  FW_Ver          Flags  Status  Radio Type
Tx_Power  Last Update  Uptime
----      -
-----
20:4c:03:bb:6e:4f  BT-AP505H  DFU App 1.4-156  0x0083  LIA      Internal
0dBm        7s          20h:9m:10sBLE Device Table [Aruba Beacons]
-----

```

```

-----
MAC                HW_Type  FW_Ver          Flags  Status  Batt(%)  RSSI
Major#  Minor#  UUID
Last Update  Uptime
----      -
-----
28:de:65:44:8a:68  ARUBA      OAD A 1.4-81    0x0081  A        --        -79
--        --        --
I:128s      30s
3c:a3:08:93:53:04  ARUBA      --              --      AH        --        -82
0          0          4152554E-F99B-4A3B-86D0-947070693A78  --        --
I:275s      --
20:4c:03:b2:79:1c  BT-AP505H  DFU App 1.3-69  0x0083  IA        ONBOARD  -91
0          0          4152554E-F99B-4A3B-86D0-947070693A78  -56        14
I:8s        18h:46m:30s
20:4c:03:44:23:58  BT-AP530   DFU App 1.4-127  0x0183  A        ONBOARD  -90
--        --        --
I:35s        13h:38m:20s
5c:f8:21:e6:d5:58  BT-AP300H  OAD B 1.2-42    0x00a3  IAH       ONBOARD  -38
0          0          4152554E-F99B-4A3B-86D0-947070693A78  -56        14
I:1s        15h:3m:30s
54:6c:0e:15:7b:5f  LS-BT20    OAD E 1.2-9     0x0001  IAH       85        -37
0          0          4152554E-F99B-4A3B-86D0-947070693A78  -60        14
I:1s        15h:26m:30s

```

```

54:6c:0e:15:6b:c6 LS-BT20 OAD E 1.2-9 0x0001 IAH 75 -35
0 0 4152554E-F99B-4A3B-86D0-947070693A78 -60 14
I:0s 15h:25m:0sBLE Device Table [Generic]
-----
MAC Address Type RSSI Last Update Device Class
Generic Filter BT-SIG Company IDs
---
-----
ac:23:3f:a9:d0:7f Public -26 I:0s eddystone, iBeacon,
minew -- 0x004C
60:12:83:1b:6d:2a Public -31 I:0s mysphera
-- 0x016CBeacons:7
Generic BLE devices:2
Total BLE devices:9Note: Battery level for LS-BT1USB devices is indicated as
USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Note: Meas. Pow. is the averaged RSSI (in dBm) when the iBeacon is
calibrated.
Note: Tx_Power is shown in dBm in the APBs section for radios that support
radio profile type 1. For all other APB radios, Tx_Power is a discrete level
from 0-15.
Status Flags:L:AP's local beacon; I:iBeacon; A:Beacon management capable
:H:High power beacon; T:Asset Tag Beacon; U:Upgrade of firmware
pending
:u:Beacon management update received
Last Update Flags:I: Device observed by internal radio
:E: Device observed by external radio
Generic Filter:S:serviceUUIDFilter; C:companyIdentifierFilter
:M:macOuiFilter; L:localNameFilter

```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-tag-report

```
show ap debug ble-tag-report {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the Bluetooth Low Energy (BLE) asset tags that are reported to the Beacon Management Console (BMC). The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Displays the BLE asset tags for a specific AP based on the AP name.
ip-addr <ip-addr>	Displays the BLE asset tags for a specific AP based on the IPv4 address.
ip6-addr <ip6-addr>	Displays the BLE asset tags for a specific AP based on the IPv6 address.



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Example

```
(host) #show ap debug ble-tag-report ap-name ap325
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ble-update-status

```
show ap debug ble-update-status
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the configuration update status for BLE devices seen by the AP. In addition, the command displays the active versus desired configuration based on the configuration received from the BMC (if any).



This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Parameter	Description
ap-name	Displays the configuration update status for BLE devices seen by the AP based on the AP name.
ip-addr	Displays the configuration update status for BLE devices seen by the AP based on the IPv4 address.
ip6-addr	Displays the configuration update status for BLE devices seen by the AP based on the IPv6 address.

Example

The output of this command displays the configuration update status for BLE devices seen by the AP. In addition, the command displays the active versus desired configuration based on the configuration received from the BMC (if any).

```
(host) #show ap debug ble-update-status ap-name ap325

BLE Device Table
-----
BLE Device MAC      Attribute  Actual/Observed
Desired/Pending
-----
-----
d0:39:72:d5:43:75  Tx Power  13                13
d0:39:72:d5:43:75  Major     1000              1000
d0:39:72:d5:43:75  Minor     1215              1215
d0:39:72:d5:43:75  UUID      5D3BCC63-BD6B-4FAF-906F-91C91519A69B
5D3BCC63-BD6B-4FAF-906F-91C91519A69B
d0:39:72:d5:43:75  DWAS      0                 0
c4:be:84:19:8b:a3  Tx Power  14                14
```

```

c4:be:84:19:8b:a3 Major 0 0
c4:be:84:19:8b:a3 Minor 0 0
c4:be:84:19:8b:a3 UUID 4152554E-F99B-4A3B-86D0-947070693A78
4152554E-F99B-4A3B-86D0-947070693A78
c4:be:84:19:8b:a3 DWAS 0 0
c4:be:84:19:ec:67 Tx Power 14 14
c4:be:84:19:ec:67 Major 0 0
c4:be:84:19:ec:67 Minor 0 0
c4:be:84:19:ec:67 UUID 4152554E-F99B-4A3B-86D0-947070693A78
4152554E-F99B-4A3B-86D0-947070693A78
c4:be:84:19:ec:67 DWAS 0 0
d0:39:72:d4:fa:9c --- Ineligible
Reason:Missing data
c4:be:84:19:ef:99 Tx Power 2 2
c4:be:84:19:ef:99 Major 1000 1000
c4:be:84:19:ef:99 Minor 1374 1374
c4:be:84:19:ef:99 UUID 09458C20-4586-4ED3-8D2F-A0842ACBD6E6
09458C20-4586-4ED3-8D2F-A0842ACBD6E6
c4:be:84:19:ef:99 Firmware 1.1-38 1.1-38
(Status:65535/0 - NotRequired)
c4:be:84:19:ef:99 DWAS 0 0
78:a5:04:15:23:35 Tx Power 13 13
78:a5:04:15:23:35 Major 1000 1000
78:a5:04:15:23:35 Minor 1222 1222
78:a5:04:15:23:35 UUID 09458C20-4586-4ED3-8D2F-A0842ACBD6E6
09458C20-4586-4ED3-8D2F-A0842ACBD6E6
78:a5:04:15:23:35 DWAS 0 0
c4:be:84:19:ec:2f Tx Power 14 14
c4:be:84:19:ec:2f Major 0 0
c4:be:84:19:ec:2f Minor 0 0
c4:be:84:19:ec:2f UUID 4152554E-F99B-4A3B-86D0-947070693A78
4152554E-F99B-4A3B-86D0-947070693A78
c4:be:84:19:ec:2f DWAS 0 0

Total beacons:7
Devices marked "Ineligible" are currently not capable of being upgraded.

```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug bss-config

```
show ap debug bss-config [ap-name <ap-name>|bssid <bssid>||essid <essid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|port <port>/<slot>]
```

Description

Shows the configuration for each BSSID of an AP. This information can be used to troubleshoot problems on an AP.

Parameter	Description
ap-name <ap-name>	Filter the AP Config table by AP name.
bssid <bssid>	Filter the AP Config table by BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
essid <essid>	Filter the AP Config table by ESSID. An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
ip-addr <ip-addr>	Filter the AP Config table by IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Filter the AP Config table by IP address by entering an IPv6 IP address in dotted-decimal format.
port <port>/<slot>	Filter the AP Config table by port and slot numbers. The slot and port numbers should be separated by a forward slash (/).

Examples

The following example shows the AP configuration table for a specific BSSID.

```
(host) #show ap debug bss-config
Aruba AP Config Table
-----
bss          ess  vlan ip          phy type fw-mode max-cl rates tx-
rates preamble mtu ---          -----
-----
status wmm
-----
00:1a:1e:11:24:c2  cera2 66 10.6.1.203  g-HT ap  tunnel  64      0x3
0xfff  enable  0  enable enable
00:1a:1e:8d:5b:11  wpa2 65 10.6.1.198  a-HT ap  tunnel  20      0x150
0xff0  -      0  enable enable
00:0b:86:9b:e5:60  guest 63 10.6.14.79  g    ap  tunnel  20      0x2
0x3fe  enable  0  enable enable
```

```

00:1a:1e:97:e5:41 voip 66 10.6.1.199 g-HT ap tunnel 20 0xc
0x14c enable 0 enable enable
00:1a:1e:11:74:a1 voip 66 10.6.1.197 g-HT ap tunnel 20 0xc
0x14c enable 0 enable enable
00:1a:1e:11:5f:11 wpa2 65 10.6.1.200 a-HT ap tunnel 20 0x150
0xff0 - 0 enable enable

```

The following example shows the AP configuration table for a specific BSSID (ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap debug bss-config

Aruba AP Config Table
-----
bss          ess          vlan ip          band/ht-mode/bandwidth
type fw-mode max-cl rates tx-rates preamble status wmm mtu
flags
---
-----
-
84:d4:7e:e6:17:50 9@hbm-535-rtp 0 1.1.1.4 5GHz/VHT/80MHz
ap tunnel 64 0x150 0xff0 - enable enable 0 D
cc:88:c7:41:64:60 8@hbm-635-psk 0 10.65.36.220 6GHz/HE/160MHz
ap tunnel 64 0x150 0xff0 enable enable enable 0
DTWx3

Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:2
Num Associations:0

Flags: a = Airslice policy; A = Airslice app monitoring; c = MBO
Cellular Data Capable BSS; d = Deferred Delete Pending; D = VLAN Discovered;
E = Enhanced-open BSS without transition mode; I = Imminent VAP Down; K =
802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS;
o = Enhanced-open transition mode open BSS; O = Enhanced-open BSS with
transition mode; r = 802.11r Enabled; t = Broadcast TWT Enabled;
T = Individual TWT Enabled; W = 802.11W Enabled; x = MBSSID Tx BSS; 3 = WPA3
BSS;

```

The output of this command includes the following information:

Column	Description
bss	Basic Service Set (BSS) identifier, which is usually the AP's MAC address.

Column	Description
ess	Extended Service Set (ESS) identifier; a user-defined name for a wireless network.
vlan	The BSSID's VLAN number.
IP	The AP's IP address.
phy 8.9.0.0) (For versions prior to ArubaOS	One of the following 802.11 types <ul style="list-style-type: none"> ■ a ■ a-HT (high-throughput) ■ g ■ g-HT (high-throughput)
band/ht-mode/bandwidth 8.9.0.0) (For versions prior to ArubaOS	The AP radio type displayed by radio band/throughput type/channel bandwidth. Possible values for each type are as follows: <ul style="list-style-type: none"> ■ band—2.4GHz, 5GHz, or 6GHz ■ ht-mode—HT, VHT, or HE ■ bandwidth—20MHz, 40MHz, 80MHz, 80+80MHz, or 160MHz
type	This column shows if the BSSID is for an access point (ap) or an air monitor (am).
fw-mode	The configured forward mode for the AP's virtual AP profile.

Column	Description
	<ul style="list-style-type: none"> ■ bridge: Bridge locally ■ split-tunnel: Tunnel to controller or NAT locally ■ tunnel: Tunnel to controller
max-cl	The maximum number of clients allowed for this BSSID.
preamble	Shows if short preambles are enabled for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using a short preamble.
MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
status	Shows if this BSSID is enabled or disabled.

Column	Description
wmm	Shows if the BSSID has enabled or disabled WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF) WMM provides prioritization of specific traffic relative to other traffic in the network.

Related Commands

Command	Description
show ap bss-table	This command shows the Basic Service Set (BSS) table of an AP.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none"> Replaced <code>phy</code> with <code>band/ht-mode/bandwidth</code> parameter in the command output. Replaced <code>g</code> and <code>a</code> with 2.4GHz and 5GHz values in the command output. Added 6GHz value in the command output for Wi-Fi 6E APs. Added <code>x</code> flag in the command output parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug bss-stats

```
show ap debug bss-stats [bssid <bssid>]
```

Description

Show debug and troubleshooting statistics from a specific BSSID of an AP.

Parameter	Description
bssid <bssid>	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The example below shows part of the output of the command `show ap debug bss-stats bssid <bssid>`.

```
(host) #show ap debug bss-stats bssid 00:1a:1e:11:5f:11
BSSID Stats
-----
BSSID Stats
-----
Parameter                               Value
-----
-----
General
-----
Transmit
-----
Tx Frames Rcvd                           972118
Tx Bcast Frames Rcvd                      4139
Tx Frames Dropped                         375241
Tx Bcast Frames Dropped                   0
Tx Frames Transmitted                     596088
Tx Bytes Rcvd                             633849487
Tx Bytes Transmitted                      593931482
Tx Time Frames Rcvd                       705492586
Tx Time Frames Dropped                    397125178
Tx Time Frames Transmitted                 308367408
Tx Success With Retry                     91875
Tx Multiple Retries                       467116
Tx Mgmt Frames                            502661
Tx Beacons Transmitted                    3528036
Tx Probe Responses                        502612
Tx Data Transmitted Retried                91867
Tx Data Transmitted                       467744
Tx Data Frames                            469457
Tx Broadcast Data Frames In               4139
Tx Data Bytes Transmitted                  580843154
Tx Data Bytes                             582581297
Tx Time Data Transmitted                   173621140
Tx Time BC/MC Data                        0
```

```

Tx Time Data dropped          4070686
Tx Time Data                  177691826
Tx Time Data (Ideal)         0
Tx Broadcast Data Frames Sent 4136
Tx Multicast Data Frames     4011
Tx DMO Multicast              0
Tx DMO Invalid                0
Tx Data Frames 12 Mbps (Mon)  0
Tx Data Frames 24 Mbps (Mon)  0
Tx Data Frames 36 Mbps (Mon)  0
Tx Data Frames 54 Mbps (Mon)  0
Tx Data Frames 72 Mbps (Mon)  0
Tx Data Frames 108 Mbps (Mon) 0
Tx Data Frames 300 Mbps (Mon) 22651
Tx Data Frames 450 Mbps (Mon) 0
Tx Data Frames 1300 Mbps (Mon) 0
Tx Data Frames 1300 Mbps+ (Mon) 0
Tx Data Bytes 12 Mbps (Mon) 0
Tx Data Bytes 24 Mbps (Mon) 0
Tx Data Bytes 36 Mbps (Mon) 0
Tx Data Bytes 54 Mbps (Mon) 0
Tx Data Bytes 72 Mbps (Mon) 0
Tx Data Bytes 108 Mbps (Mon) 0
Tx Data Bytes 300 Mbps (Mon) 34300555
Tx Data Bytes 450 Mbps (Mon) 0
Tx Data Bytes 1300 Mbps (Mon) 0
Tx Data Bytes 1300 Mbps+ (Mon) 0
Tx 6 Mbps                      11
Tx HT 130 Mbps                  22651
Tx WMM [BE]                     22651
Tx UAPSD OverflowDrop           0
Tx Mgmt Bytes                    547
...

```

The output of this command includes the following information:

Column	Description
Tx Frames Rcvd	Number of transmitted frames that were received.
Tx Bcast Frames Rcvd	Number of transmitted broadcast frames that were received.
Tx Frames Dropped	Number of transmitted frames that were dropped.
Tx Bcast Frames Dropped	Number of transmitted broadcast frames that were dropped.
Tx Frames Transmitted	Number of frames successfully transmitted.
Tx Bytes Rcvd	Number of transmitted bytes received.

Column	Description
Tx Bytes Transmitted	Number of transmitted bytes.
Tx Time Frames Rcvd	Number of times transmitted frames were received.
Tx Time Frames Dropped	Number of times transmitted frames were dropped.
Tx Time Frames Transmitted	Number of times frames were transmitted.
Tx Success With Retry	Number of frames that were successfully transmitted after being retried.
Tx Multiple retries	Number of frames that were successfully transmitted after being retried multiple times.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Beacons Transmitted	Number of beacons transmitted.
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Transmitted Retried	Number of retried data frames.
Tx Data Transmitted	Number of transmitted data frames.
Tx Data Frames	Number of transmitted data frames.
Tx Broadcast Data Frames In	Number of broadcast data frames received by the AP from wired interface to be transmitted in the air.
Tx Data Bytes Transmitted	Total data bytes received by an AP from its wired interface to be transmitted over the air.
Tx Data Bytes	Total data bytes transmitted by the AP over the air.
Tx Time BC/MC Data	Total time spent transmitting broadcast/multicast frames.
Tx Time Data dropped	Total time spent transmitting dropped frames.
Tx Time Data	Total time spent sending frames received for transmission, including the frames that were dropped after retrying.
Tx Broadcast Data Frames Sent	Broadcast data frames transmitted by the AP.
Tx Multicast Data Frames	Multicast data frames transmitted by the AP.

Column	Description
Tx DMO Multicast	<p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO Invalid	<p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO Converted	<p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO Replicated	<p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO Dropped	<p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO No Client	<p>Number of times no client was found for an association-ID indicated by the frame. (This value is typically normally 0.)</p> <p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.</p>
Tx DMO No BSSID	<p>Number of times the BSSID indicated by the frame was not found. (This value is typically normally 0.)</p> <p>NOTE: This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may</p>

Column	Description
	also increment for Instant APsin bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx Unicast Data Frames	Number of transmitted unicast data frames.
Tx RTS Success	Number of Ready To Send (RTS) frames successfully transmitted.
Tx RTS Failed	Number of Ready To Send (RTS) frames that were not successfully transmitted
Tx CTS Frames	Number of Clear-to-Send (CTS) frames transmitted.
Tx Dropped After Retry	Number of frames dropped after an attempted retry.
Tx Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Tx Missed ACKs	Number of retries triggered because an acknowledgement was not received.
Tx EAPOL Frames	Number of EAPOL frames transmitted
TX STBC Frames	Number of transmitted frames with Space-time block coding (STBC) enabled.
TX LDPC Frames	Number of transmitted frames with Low Density Parity Check (LDPC) enabled.
Tx WMM	<p>Number of Wi-fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command.</p> <ul style="list-style-type: none"> ■ Tx WMM [BE]: Best Effort ■ Tx WMM [BK]: Background ■ Tx WMM [VO]: VoIP ■ Tx WMM [VI]: Video
Tx Data <value> Mbps	Number of frames transmitted at the specified rate, (Mbps).
Tx Data Bytes <value> Mbps	Number of bytes of data transmitted at the specified rate, (Mbps).
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.

Column	Description
Tx Mgmt Bytes	Total management frame bytes transmitted.
Tx Beacons Bytes	Total number of Beacon frame bytes transmitted.
Tx AMSDU pkt count	Total number of AMSDU bytes transmitted.
Tx Data Frames/Bytes 24 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (12-24)
Tx Data Frames/Bytes 36 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (24-36)
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9

Column	Description
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI (HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI (FULL)	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Rx Last SNR	The last recorded signal-to-noise ratio.
Rx Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.

Column	Description
Rx Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Frames Received	Number of frames received.
Rx retry frames	Number of retried frames received.
Rx data frames retried	Number of retried data frames received.
Rx Data Frames	Number of data frames received.
Rx Data Bytes	Number of data bytes received.
Rx Time Data	Total time spent on frames successfully received.
Rx Duplicate Frames	Number of duplicate frames received.
Rx Broadcast Data Frames	Number of broadcast frames received.
Rx Multicast Data Frames	Number of multicast frames received.
Rx Unicast Data Frames	Number of unicast frames received.
Rx Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
Control Frames	Number of control frames received.
Frames To Me	Number of frames received that are addressed to the specified BSSID.
Bytes To Me	Number of bytes received that are addressed to the specified BSSID.
Time To Me	Total time spent receiving frames sent to a specified BSSID.
Rx Probe Requests	Number of probe requests received.

Column	Description
RX PS Poll Frames	Power-Save Poll (PS-Poll) frames received. When a client exits a power-saving mode, it transmits a PS-Poll frame to the AP to retrieve any frames buffered while it was in power-saving mode.
RX STBC Frames	Number of received frames with STBC enabled.
RX LDPC Frames	Number of received frames with LDPC enabled.
Rx Data <value> Mbps	Number of frames received at the specified rate, (Mbps).
Rx Data Bytes <value> Mbps	Number of bytes of data received at the specified rate, (Mbps).

Related Commands

Command	Description
show ap bss-table	This command shows the Basic Service Set (BSS) table of an AP.

Command History

Release	Modification
ArubaOS 8.3.0.0	The output of this command now includes MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug bucketmap-state

```
show ap debug bucketmap-state
  essid <ssid>
  filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr
<ip6-addr>}
  uac {bucket <bucket> | dormant {ssid <ssid> | filter-by {ap-name <ap-name> |
  bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
  verbose {ssid <ssid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr
<ip-addr> | ip6-addr <ip6-addr>}} | uac-ip <uac-ip> | uac-ip6 <uac-ip6>}
  verbose {ssid <ssid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr
<ip-addr> | ip6-addr <ip6-addr>} | uac {bucket <bucket> | dormant {ssid <ssid> |
filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-
addr>}}}}}
```

Description

This command shows clients in different buckets.

Parameter	Description
ssid <ssid>	Shows clients filtered by ESSID.
filter-by {ap-name <ap-name> bssid <bssid> ip-addr <ip-addr> ip6-addr <ip6-addr>}	Shows clients filtered by name of AP, BSSID, IP address or IPv6 address.
uac {bucket <bucket> dormant {ssid <ssid> filter-by {ap-name <ap-name> bssid <bssid> ip-addr <ip-addr> ip6-addr <ip6-addr>} verbose {ssid <ssid> filter-by {ap-name <ap-name> bssid <bssid> ip-addr <ip-addr> ip6-addr <ip6-addr>}} uac-ip <uac-ip> uac-ip6 <uac-ip6>}}	Shows clients filtered by bucket index, dormancy, IP address, or IPv6 address.
verbose {ssid <ssid> filter-by {ap-name <ap-name> bssid <bssid> ip-addr <ip-addr> ip6-addr <ip6-addr>} uac {bucket <bucket> dormant {ssid <ssid> filter-by {ap-name <ap-name> bssid <bssid> ip-addr <ip-addr> ip6-addr <ip6-addr>}}}}	Shows clients filtered by bucket index, dormancy, IP address, or IPv6 address

Example

Access the CLI and use the following command to show clients filtered by the ESSID **test**:

```
(host) [mynode] #show ap debug bucketmap-state essid test

Essid "test"
Number of updates 1; Time since last update 1h:19m:24s
Activations: New Bmap=0, Node Down=0
Bucketmap State
-----
Index  UAC                               status
-----  ---  -----
0      10.15.146.3 (self) Up
1      10.15.146.4 Up
2      10.15.146.5 Up
3      10.15.146.6 Up
Stations in buckets for Essid SriniZone1TestEssid
-----
BucketIndex  MAC  BSSID  AID  AP Name  UAC IP
-----  ---  -----  ---  -----  -----
Total Stations=0 Total Active=0 Total Dormant=0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug client-death-reason-counters

show ap debug client-death-reason-counters

Description

Shows the aggregate client death reason counters.

Examples

The output of the command below shows client death reason counters.

```
(host) #show ap debug client-death-reason-counters
Death Reason Counters
-----
Name                Value
-----
```

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-info

```
show ap debug client-info <client-mac>
```

Description

This command displays all the details of a specific client in WLAN driver, for client debugging.

Parameter	Description
client-mac	The client MAC address.

Examples

The example below displays the output of the `show ap debug client-info` command:

```
(host) [mynode] #show ap debug client-info client-mac 78:31:c1:be:93:74
```

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
802.11ax platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-kickout-logs

```
show ap debug client-kickout-logs {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>} {radio <radio>}
```

Description

This command displays the last 12 occurrences of the client kickout (deauthentication) logs per radio that occurs due to consecutive Tx failures on APs.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name> ip-addr <ip-addr> ip6-addr <ip6-addr>	Shows debug client kickout logs for specified AP name, IPv4 address, or IPv6 address.
radio <radio>	Shows information for a specific radio type. The valid values are 0, 1, and 2.



This command is supported in 530 Series, 550 Series, 630 Series, and 650 Series access points.

Example

The following example shows the client kickout logs on AP-535.

```
(host) [mynode] #show ap debug client-kickout-logs ap-name ap535 radio 0
Client kickout due to consecutive Tx failures
=====
Last 12 occurrence (most recent first)
-----
client-mac: 00:01:5d:8d:50:46
BSSID: 00:4e:35:c4:dc:f0
Association ID: 7
Total association time (ms): 221820
Total Tx frames transmitted: 10538
Consecutive Tx failure...
Failure counts per frame types
RTS: 0
BAR: 457
Trigger: 0
AMPDU: 55
Non-AMPDU: 0
Kickout thresh: 512
Elapsed time (ms): 36598
Fake sleep...
```

Number of entering fake sleep: 2
Number of timeout: 2
Rx event count during Tx failure: 0
Last Tx rate (Kbps): 405000
ACK SNR history (dB: ms before kickout)
22: 221730
57: 95730
43: 74730
35: 64730
22: 54730
Last ACK SNR (dB): 18
Rx SNR history (dB: ms before kickout)
29: 149730
63: 95730
49: 74730
38: 64730
20: 41730
Last Rx SNR (dB): 20
Time of kickout: UTC 2021-12-17 04:07:06

client-mac: 00:01:5d:8d:50:83
BSSID: 00:4e:35:c4:dc:f0
Association ID: 68
Total association time (ms): 218840
Total Tx frames transmitted: 10210
Consecutive Tx failure...
Failure counts per frame types
RTS: 0
BAR: 456
Trigger: 0
AMPDU: 56
Non-AMPDU: 0
Kickout thresh: 512
Elapsed time (ms): 36538
Fake sleep...
Number of entering fake sleep: 2
Number of timeout: 2
Rx event count during Tx failure: 0
Last Tx rate (Kbps): 540000
ACK SNR history (dB: ms before kickout)
22: 218680
57: 95680
43: 74680
32: 64680
22: 54680
Last ACK SNR (dB): 18
Rx SNR history (dB: ms before kickout)
27: 218680
63: 95680
49: 74680
38: 64680
23: 41680
Last Rx SNR (dB): 19
Time of kickout: UTC 2021-12-17 04:07:06

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.
ArubaOS 8.6,0,17 and 8.7,1.9	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug client-mgmt-counters

show ap debug client-mgmt-counters

Description

This command shows the message counters. This command shows the numbers of each type of message sent from a client to an AP. Use this information to troubleshoot problems on an AP.

Examples

The following example shows the client management counters.

```
(host) [mynode] #show ap debug client-mgmt-counters

Counters
-----
Name                                     Value
-----
41228                                     3
Tunnel DACL                              7
STM Restart Notification to Auth         1
Associations Dropped Due to Auth Throttling 0
PubSub Messages Rcvd                     992
User Mon Messages                         0
Auth .lx Queue: High, Pending           450, 0
Reg timer calls                           141274
BSS publish Failures                     0
Tunnel Timeouts                           0
Unreg/Wipeout Requests                   0 0
Auth Resp for unknown sap                 0
Auth enet Resp Tout                      0
SOS Rx Msg Count: tunop ctrl dtun_data tun_data misc
0 0 0 0 0 0 0 0
Received Client Ageout Messages from APs  0
Received stale Entries                    0
Received stale Entries in Deauth (Deauths from clients) 0
Processed stale Entries in Deauth         0
Stale entry error - BSS not found         0
Stale entry error - STA not found in Deauth 0
Stale entry error - failed to clear STA in Deauth 0
Stale entry error - Deauth bad length     0
Stale entry error - special handling      0
Sta down: total flag_unmatch not_assoc papi_send papi_ok papi_fail
0 0 0 0 0 0
Sta up: total flag_unmatch not_assoc papi_send papi_ok papi_fail
0 0 0 0 0 0
AMSDU Updates sent to SOS from STM        0
Invalid tunnel-id (0)                     0
HBT tunnel not found on timeout           0
AID-MAC mismatch                          0
```

Related Commands

Command	Description
show ap remote debug client-mgmt-counters	This command shows the number of each type of message from the clients of an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-stats

```
show ap debug client-stats
  client-mac <client_mac> [advanced]
```

Description

This command shows the detailed statistics about a client from an AP.

Parameter	Description
client-mac <client_mac> [advanced]	Shows detailed statistics about a specified client MAC.
advanced	Shows additional statistics.

Example

The following command shows additional statistics for packets received from and transmitted to a specified client.

```
(host) [mynode] #show ap debug client-stats client-mac 00:19:7e:89:fa:e7
advanced

Station Stats
-----
Parameter          Value
-----
-----
General Per-radio Statistics
Transmit specific Statistics
Frames Rcvd For TX 22
Tx Frames Dropped  0
Frames Transmitted 22
Success With Retry  1
Tx Mgmt Frames      2
Tx Probe Responses  0
Tx Data Frames      20
Tx CTS Frames       0
Dropped After Retry 0
Dropped No Buffer    0
Missed ACKs         1
Long Preamble       22
Short Preamble       0
Tx EAPOL Frames     13
Tx 6 Mbps           15
Tx 48 Mbps           5
Tx 54 Mbps           2
Tx WMM [VO]         15
UAPSD OverflowDrop  0
TX LDPC Frames      0
Tx Data Priority [BE] 6283
```

Tx Data Frames	12 Mbps	(Mon)	0
Tx Data Frames	24 Mbps	(Mon)	0
Tx Data Frames	36 Mbps	(Mon)	0
Tx Data Frames	54 Mbps	(Mon)	0
Tx Data Frames	72 Mbps	(Mon)	0
Tx Data Frames	108 Mbps	(Mon)	0
Tx Data Frames	300 Mbps	(Mon)	6283
Tx Data Frames	450 Mbps	(Mon)	0
Tx Data Frames	1300 Mbps	(Mon)	0
Tx Data Frames	1300 Mbps+	(Mon)	0
Tx Data Bytes	12 Mbps	(Mon)	0
Tx Data Bytes	24 Mbps	(Mon)	0
Tx Data Bytes	36 Mbps	(Mon)	0
Tx Data Bytes	54 Mbps	(Mon)	0
Tx Data Bytes	72 Mbps	(Mon)	0
Tx Data Bytes	108 Mbps	(Mon)	0
Tx Data Bytes	300 Mbps	(Mon)	9510308
Tx Data Bytes	450 Mbps	(Mon)	0
Tx Data Bytes	1300 Mbps	(Mon)	0
Tx Data Bytes	1300 Mbps+	(Mon)	0
Tx 6 Mbps			5
Tx HT 130 Mbps			6283
Tx WMM [BE]			6283
Tx UAPSD OverflowDrop			0
Tx AMSDU pkt count			0
Tx EAPOL Frames Rcvd			0
Tx EAPOL Frames Dropped			0
Tx Data Frames MCS 7 :			6283
Tx Data Frames MCS :			6283
Tx Data Frames NSS2 :			6283
Tx Data Frames Long-GI (FULL) :			6283
Tx Data Frames BW 20 :			6283

		Receive specific Statistics	
Last SNR		31	
Last SNR CTL0		28	
Last SNR CTL1		25	
Last SNR CTL2		22	
Last ACK SNR		32	
Last ACK SNR CTL0		30	
Last ACK SNR CTL1		28	
Last ACK SNR CTL2		21	
Last ACK SNR EXT0		5	
Last ACK SNR EXT1		4	
Frames Received		2932	
Rx Data Frames		2930	
Null Data Frames		2879	
Rx Mgmt Frames		1	
PS Poll Frames		0	
Rx 6 Mbps		14	
Rx 12 Mbps		6	
Rx 18 Mbps		5	
Rx 24 Mbps		2	
Rx 36 Mbps		13	
Rx 48 Mbps		1162	
Rx 54 Mbps		1730	
Rx WMM [BE]		39	

The output of this command includes the following information:

Column	Description
Frames Rcvd For TX	Number of frames received for transmission.
Tx Frames Dropped	Number of transmission frames that were dropped.
Frames Transmitted	Number of frames successfully transmitted.
Success With Retry	Number of frames that were transmitted after being retried.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Frames	Number of transmitted data frames.
Tx CTS Frames	Number of clear-to-send (CTS) frames transmitted.
Dropped After Retry	Number of frames dropped after an attempted retry.
Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Missed ACKs	Number of missed acknowledgements (ACKs)
Long Preamble	Number of frames sent with a long preamble.
Short Preamble	Number of frames sent with a short preamble.
Tx EAPOL Frames	Number of Extensible Authentication Protocol over LAN (EAPOL) frames transmitted.
Tx <n> Mbps	Number of frames transmitted at <n> Mbps, where <n> is a value between 6 and 300.
Tx WMM	<p>Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command.</p> <ul style="list-style-type: none"> ▪ Tx WMM [BE]: Best Effort ▪ Tx WMM [BK]: Background ▪ Tx WMM [VO]: VoIP ▪ Tx WMM [VI]: Video
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.

Column	Description
Tx Data Frames/Bytes 24 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (12-24)
Tx Data Frames/Bytes 36 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (24-36)
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate

Column	Description
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI (HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI (FULL)	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Last SNR	The last recorded signal-to-noise ratio.
Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.
Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.

Column	Description
Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Frames Received	Number of frames received.
Rx Data Frames	Number of data frames received.
Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
PS Poll Frames	Number of power save poll frames received.
Rx <n> Mbps	Number of frames received at <n> Mbps, where <n> is a value between 6 and 300.
Tx WMM	<p>Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command.</p> <ul style="list-style-type: none"> ▪ Tx WMM [BE]: Best Effort ▪ Tx WMM [BK]: Background ▪ Tx WMM [VO]: VoIP ▪ Tx WMM [VI]: Video

Related Commands

Command	Description
show ap client status	This command shows the current status of a specific client.

Command History

Release	Modification
ArubaOS 8.3.0.0	The output of this command now includes MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-table

```
show ap debug client-table [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
```

Description

This command shows clients associated with an AP. The **Tx_Rate**, **Rx_Rate**, **Last_ACK_SNR**, and **Last_Rx_SNR** columns shown in the output of this command show valuable troubleshooting information for clients trying to connect to a specific AP. Use this command to verify that the transmit (Tx_Rate) and receive (Rx_Rate) rates are not too low, and that the SNR is acceptable.

Parameter	Description
ap-name <ap-name>	Filters the client table by AP name.
bssid <bssid>	Filters the client table by BSSID. This will print clients on top from given BSSID.
ip-addr <ip-addr>	Filters the client table by AP IP address.
ip6-addr <ip6-addr>	Filters the client table by AP IPv6 address.

Examples

The example below displays the AP configuration table for a specific BSSID. In this example, the output is divided into multiple sections to better fit on the pages of this document. In the actual CLI, it appears in a single, long table.

```
(host) #show ap debug client-table ap-name apname1
Client Table
-----
MAC              ESSID              BSSID              Assoc_State  HT_
State  AID
---  ---
-  ---
00:10:18:a9:7c:48  essidname1        6c:f3:7f:e7:5c:90  Associated
cAWvSseM  0x1

PS_State  UAPSD              Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate
-----  -----
Awake     (0,0,0,0,N/A,0)  799      1377     0         48           1300
1053

Last_ACK_SNR  Last_Rx_SNR  TX_Chains  Tx_Timestamp
-----  -----
32         47          3[0x7]     Sun Jul 21 11:05:50 2013
```

```

Rx_Timestamp           MFP Status (C,R)   Idle time   Client health (C/R)
-----
Sun Jul 21 11:05:50 2013  (0,0)       119         90/90

UAPSD: (VO,VI,BK,BE,Max SP,Q Len)
HT  Flags: A - LDPC Coding; W - 40MHz; S - Short GI 40; s - Short GI 20
D - Delayed BA; G - Greenfield; R - Dynamic SM PS
Q - Static SM PS; N - A-MPDU disabled; B - TX STBC
b - RX STBC; M - Max A-MSDU; I - HT40 Intolerant
VHT Flags: C - 160MHz; c - 80MHz; V - Short GI 160; v - Short GI 80
E - Beamformee; e - Beamformer
HT_State shows client's original capabilities (not operational capabilities)

```

The output of this command includes the following information:

Parameter	Description
MAC	MAC address of a client.
ESSID	ESSID used by the client. An ESSID is a user-defined name for a wireless network.
BSSID	BSSID for the client.
Assoc_State	The associated state column shows whether or not the client is currently authorized and/or associated with the AP.
HT_State	Shows information about the client's high-throughput or very-high throughput transmission type. The description for each of the flags that can appear in this column follows the output of the command. <ul style="list-style-type: none"> ▪ A - LDPC Coding ▪ W - 40MHz ▪ S - Short GI 40 ▪ s - Short GI 20 ▪ D - Delayed BA ▪ G - Greenfield ▪ R - Dynamic SM PS ▪ Q - Static SM PS ▪ N - A-MPDU disabled ▪ B - TX STBC ▪ b - RX STBC ▪ M - Max A-MSDU ▪ I - HT40 Intolerant ▪ C - 160MHz ▪ c - 80MHz ▪ V - Short GI 16 ▪ v - Short GI 80 ▪ E - Beamformee

Parameter	Description
	<ul style="list-style-type: none"> ▪ e - Beamformer
AID	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
PS_State	Powersave state, showing if the AP is in the awake or power-save state.
UAPSD	<p>Shows the U-APSD queue statuses in the following comma-separated format: (<VO>,< VI>,< BK>, <BE>,< Max SP>,<Q Len>).</p> <ul style="list-style-type: none"> ▪ VO: If 1, UAPSD is enabled for the VoIP access category. If UAPSD is disabled for this access category, this value is 0. ▪ VI: If 1, UAPSD is enabled for the Video access category. If UAPSD is disabled for this access category, this value is 0. ▪ BK: If 1, UAPSD is enabled for the Background access category. If UAPSD is disabled for this access category, this value is 0. ▪ BE: If 1, UAPSD is enabled for the Best Effort access category. If UAPSD is disabled for this access category, this value is 0. ▪ Max SP: The maximum service period is the number of frame sent per trigger packet. This value is value can be 0, 2, 4 or 8. ▪ Q Len: The number of frames currently queued for the client, from 0 to 16 frames.
Tx_Pkts	Number of packets transmitted from the AP to the client.
Rx_Pkts	Number of packets the AP received from the client.
PS_Qlen	Number of packets in the power-save queue length.
Tx_Retries	Number of packets that the AP had to resend to the client due to an initial transmission failure.
Tx_rate	Rate at which last packet was sent to the client (in Mbps).
Rx_rate	Rate at which last packet was received from the client (in Mbps).
Last_ACK_SNR	SNR of the last acknowledge packet sent by the client.
Last_Rx_SNR	SNR of the last data packet received from the client.
TX_Chains	The first digit in this value indicates the number of transmission chains on the radio currently in use and the number in brackets shows which of the chains are active.

Parameter	Description
	<p>The current status of each chain is indicated by a single-digit binary number; 1 if the chain is active, and 0 if it is inactive. In the example output above (2 [0x5]), two chains are active; chain one and chain three.</p> <ul style="list-style-type: none"> ▪ chain one: 1 (active) ▪ chain two: 0 (inactive) ▪ chain three: 1 (active) <p>In the example above, the chain would generate the value 101, which translates to the hexadecimal number 5. If all three chain were active, it would generate the value 111, (the hexadecimal number 7), and would appear in the CLI output as 3 [0x7].</p>
Tx_timestamp	Date and time the last packet was sent to the client.
Rx_timestamp	Date and time the last packet was received from the client.
MFP status	Client is 802.11W capable/802.11W is enabled on radio.
Idle Time	Number of seconds elapsed since a packet was received from the client.
Client Health	<p>Shows the health of the client and the AP radio in the format <client_health>/<AP-health>. These values report the quality of link between the client and the radio,</p> <p>An AP's client health is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries. A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.</p>

Related Commands

Command	Description
rf arm-profile	This command enables ClientMatch.
show ap arm client-match neighbors	This command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Command	Description
<u>show ap arm virtual-beacon-report</u>	This command displays the virtual beacon report for an AP with a specific IP or MAC address.
<u>show ap arm client-match unsupported</u>	This command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered.
<u>show ap arm client-match summary</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match history</u>	This command shows the history of AP association changes triggered by the client match feature.
<u>show ap arm client-match restriction-table</u>	This command displays the list of clients that ClientMatch has restricted from the specified AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-trace

```
show ap client-trace
  {ap-name <ap-name>|clients|ip-addr <ip-addr>}|ip6-addr <ip6-addr>}<mac>
```

Description

This command shows the counts of different types of management data frames traced from a client MAC address. You must issue the command only under the guidance of Aruba technical support. This command is supported on 100 Series, 120 Series, and 130 Series access points only.

Parameter	Description
ap-name <ap-name>	Shows counts for an AP with a specific name.
clients	Shows all registered clients in the AP.
ip-addr <ip-addr>	Shows counts for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	Shows counts for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.
<mac>	MAC address of the client.

Example

The following example shows an AP model that does not support the `show ap debug client-trace` command.

```
(host) #show ap debug client-trace ap-name ap-205
The AP platform does not support the command
```

Related Commands

Command	Description
ap debug client-trace start	Use this command to trace management packets from a client MAC address.
ap debug client-trace stop	Use this command to stop tracing management packets from a client MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug client-trace clients

```
show ap debug client-trace clients {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows debug client trace for all registered clients in an AP.

Parameter	Description
ap-name <ap-name>	Shows debug client trace for all registered clients in an AP for specified AP name.
ip-addr <ip-addr>	Shows debug client trace for all registered clients in an AP for specified IP address.
ip6-addr <ip6-addr>	Shows debug client trace for all registered clients in an AP for specified IPv6 address.

Example

The following example shows an AP named ap-205 does not support the show ap debug client-trace clients command:

```
(host) [mynode] #show ap debug client-trace clients ap-name ap-205  
The AP platform do not support the command
```

Related Commands

Command	Description
ap deploy-profile	This command applies the AP deployment policy to the default AP group, and/or to the list of AP MAC addresses included in the UAP blacklist table, and/or to the specified IP address range. The AP deployment policy redirects the applicable APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug cluster-counters

show ap debug cluster-counters

Description

This command shows the controller cluster statistics.

Examples

The output of the command below shows cluster statistics.

```
(host) (config) #show ap debug cluster-counters

STM Cluster Debug Counters
-----
Name                                     Value
----                                     -
UAC BSS Adds, Add Failures              0 0
UAC BSS: Role Cleared, Deletes, Delete Failures 0 0 0
Standby UAC BSS Adds, Add Failures      0 0
Dormant STA: Success, No Bmap on add, Fails, Defer Add 6, 0, 0 0
STAs emptied : UAC, Standby UAC, STA_negve SBY_negve 0, 6, 0 0
Down Node: not found, update bmap, not in bmap, self not in bmap 6, 2, 0 0
Standby Activations, Activation Errors, Not dormant 0 0 0
Active De-activations: No STA, No SAP, No SAP_STA 0 0 0 0 0
SOS punted frames ignored at UAC        0
Cluster Disable Events                  2
Bucketmap Events when Cluster Disabled  0
Bucketmap Create Events, SAPM bmap errors 12 3
AAC SAP Stby to Active: Requests, moves, empty 5 1 4
AAC Enet Stby to Active: Requests, moves, empty 5 0 5
Dormant STA: Skip Clear, Ageout         0 6
AUTH restart Clear AP events            0
CBSS DEL Ignored: AAC, SBY-AAC         5 38
CBSS Not found count                    0
```

Related Commands

Command	Description
stm	This command is used to manually disconnect a client from an AP or control the blacklisting/denylisting of clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show ap cluster-node-state

show ap cluster-node-state

Description

This command shows the nodes state of a cluster.

Example

The output of this command shows the state of the nodes in a cluster:

```
(host) (config) #show ap debug cluster-node-state

Cluster Name "multiZone1"; Redundancy=Yes; Cluster AP Limit=0
Cluster Nodes
-----
Index  Node IP                Status  Duration since Last Update
-----  -----
0      10.15.146.3 (self)  Up      3d:18h:44m:26s
1      10.15.146.4           Up      3d:18h:40m:2s
2      10.15.146.6           Up      3d:18h:40m:2s
3      10.15.146.5           Up      3d:18h:40m:2s
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show ap debug config-msg-history

```
show ap debug config-msg-history {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows recent configuration messages sent and received by an AP.

Parameter	Description
ap-name <ap-name>	Shows recent configuration messages sent and received by an AP for specified AP name.
ip-addr <ip-addr>	Shows recent configuration messages sent and received by an AP for specified IP address.
ip6-addr <ip6-addr>	Shows recent configuration messages sent and received by an AP for specified IPv6 address.

Examples

The following example shows the configuration message history for the AP named ap-205:

```
(host) [mynode] #show ap debug config-msg-history ap-name ap-205

Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=LOG_CONFIG len=151
peer=192.192.189.1 seq_num=3 resps_sent=1
0400000092040000001405C0C0BD0104575BE5D404000000307020107020104000000060400
0002080400000004040000000004000001880400000004040000
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=MONITORING_MSG_
CONFIG len=59 peer=192.192.189.1 seq_num=4 resps_sent=1
0400000036040000001D05C0C0BD0104575BE5D40400000004020102C7027F025502FC02FF02
E4023F020002F9021F0200020002000200020002000200
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=ESSID_LIST len=94
peer=192.192.189.1 seq_num=5 resps_sent=1
0400000059040000002705C0C0BD0104575BE5D4040000000504000000050000086172756261
2D617000000A61727562612D6D657368000008656D706C6F7965
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=MCELL len=28
peer=192.192.189.1 seq_num=6 resps_sent=1
0400000017040000003905C0C0BD0104575BE5D40400000006070201
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0
peer=0.0.0.0 seq_num=0
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0
peer=0.0.0.0 seq_num=0
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0
peer=0.0.0.0 seq_num=0
```

```
Sat Jun 11 02:20:05 2016(1779220 secs ago): RCVD REQ type=REG_DOM_INFO
len=1787 peer=192.192.189.1 seq_num=0 resps_sent=1
04000006F6040000003505C0C0BD0104575BE5D4040000000070201021602240228022C0230
02340238023C024002640268026C0270027402840288028C0290
Sat Jun 11 02:20:05 2016(1779220 secs ago): RCVD REQ type=CONFIG len=3508
peer=192.192.189.1 seq_num=1 resps_sent=1
0400000DAF04000000F05C0C0BD0104575BE5D404000000010400000000400000005070201
0200040000000504000001A804000000000400000001040000003
Sat Jun 11 02:20:12 2016(1779213 secs ago): RCVD REQ type=CONFIG len=2291
peer=192.192.189.1 seq_num=2 resps_sent=1
04000008EE04000000F05C0C0BD0104575BE5D4040000000204000000030400000034040000
000004000000000400000000040000000107020104575BE5D400
Fri Jul 1 15:00:18 2016(5607 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2958 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B8E045776F60205FFFFFF0005BFBF
BF000000000000
Fri Jul 1 15:10:18 2016(5007 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2959 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B8F045776F85A05FFFFFF0005BFBF
BF000000000000
Fri Jul 1 15:20:18 2016(4407 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2960 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B90045776FAB205FFFFFF0005BFBF
BF000000000000
Fri Jul 1 15:30:18 2016(3807 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2961 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B91045776FD0A05FFFFFF0005BFBF
BF000000000000
Fri Jul 1 15:40:18 2016(3207 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2962 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B92045776FF6205FFFFFF0005BFBF
BF000000000000
Fri Jul 1 15:50:18 2016(2607 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2963 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B9304577701BA05FFFFFF0005BFBF
BF000000000000
Fri Jul 1 16:00:18 2016(2007 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2964 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B94045777041205FFFFFF0005BFBF
BF000000000000
Fri Jul 1 16:10:18 2016(1407 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2965 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B95045777066A05FFFFFF0005BFBF
BF000000000000
Fri Jul 1 16:20:18 2016(807 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2966 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B9604577708C205FFFFFF0005BFBF
BF000000000000
Fri Jul 1 16:30:18 2016(207 secs ago): SENT REQ type=KEEPALIVE len=45
peer=192.192.189.1 seq_num=2967 num_attempts=1 rtt=0 secs
0400000028040000000205BFBFBF040000000004000000B970457770B1A05FFFFFF0005BFBF
BF000000000000
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug counters

```
show ap debug counters {ap-name <ap-name>|bssid <bssid>|group <group>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows AP reboot/bootstrap counters and crash information for an individual AP or AP group, or all APs referenced on the controller.

Parameter	Description
ap-name <ap-name>	Shows debug counters for an AP with a specified name.
bssid <bssid>	Shows debug counters for a specific BSSID. The BSSID is usually the AP's MAC address.
group <group>	Shows debug counters for an AP group.
ip-addr <ip-addr>	Shows debug counters for an AP with a specified IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	Shows debug counters for an AP with a specified IPv6 address by entering an IPv6 address in the dotted-decimal format.

Example

The output of this command shows how many times each AP has rebooted (a hard boot) or bootstrapped (a soft boot), the number of configuration changes sent and acknowledged by that AP, and whether or not the AP rebooted due to a kernel crash.

In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, it will appear in a single, long table.

```
(host) #show ap debug counters group corp1
AP Counters
-----
Name   Group  IP Address  Configs Sent  Configs Acked  AP Boots Sent
-----
AL1    corp1  10.6.1.209  1597          1597           0
AL10   corp1  10.6.1.198  165           165            0
AL12   corp1  10.6.1.200  195           195            0
AL15   corp1  10.6.1.197  1580          1580           0
AL16   corp1  10.6.1.199  73            73             0
AL19   corp1  10.6.1.212  8             8              0

AP Boots Acked  Bootstraps (Total)  Reboots  Crash
-----
0             1                (1)      0      N
```

```

0          2          (2)          1          Y
0          1          (1)          0          N
0          1          (1)          0          N
0          1          (1)          0          N
0          1          (1)          0          N
Total APs :6

```

The output of this command includes the following information:

Column	Description
Name	Name of the AP.
Group	Name of the AP's group.
IP Address	IP address of the AP.
Configs sent	Number of times configuration changes have been sent to the AP.
Configs Acked	Number of times that the AP has acknowledged receiving a configuration change.
AP Boots Sent	Number of times reboot requests have been sent to the AP.
AP Boots Acked	Number of times that the AP has acknowledged receiving a reboot request.
Bootstraps	Number of times the AP bootstrapped since AP reboot. Bootstraps are also known as "soft" restarts.
Total Bootstraps	Total number of times the AP bootstrapped since AP image upgrade.
Reboots	Number of times power to the AP cycled off and then on again since image upgrade. Reboots also known as "hard" restarts.
Crash	Indicates whether or not the AP was rebooted due to a kernel crash. Use show ap debug crash-info command to view the crash signature.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug crash-info

```
show ap debug crash-info {ap-name <ap-name>|ip-addr <ip-addr>
ip6-addr <ip6-addr>}
```

Description

This command shows crash log information (if it exists) for an individual AP. The stored information is cleared from the flash after the AP reboots.

Parameter	Description
ap-name <ap-name>	Shows crash information for an AP with a specified name.
ip-addr <ip-addr>	Shows crash information for an AP with a specified IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	Shows crash information for an AP with a specified IPv6 address by entering an IPv6 address in the dotted-decimal format.

Example

The output of this command shows a partial sample crash log information for an AP named **MyAP**:

```
(host) #show ap debug crash-info ap-name MyAP
<4>ArubaOS Version x.x.x.x (build xxxx / label #xxxx)
<4>Built by p4build@cartman on 2012-07-29 at 14:44:06 PST (gcc version x.x.x
Cavium Networks Version: 1.4.0, build 58)
<4>CVMSEG size: 2 cache lines (256 bytes)
<4>Setting flash physical map for 16MB flash at 0x1ec00000
<4>Determined physical RAM map:
<7>On node 0 totalpages: 16384
<7> DMA zone: 16384 pages, LIFO batch:3
<7> DMA32 zone: 0 pages, LIFO batch:0
<7> Normal zone: 0 pages, LIFO batch:0
<7> HighMem zone: 0 pages, LIFO batch:0
<4>Primary instruction cache 32kB, virtually tagged, 4 way, 64 sets,
linesize 128 bytes.
<4>Primary data cache 16kB, 64-way, 2 sets, linesize 128 bytes.
<4>Using 500.000 MHz high precision timer. cycles_per_jiffy=1000000
<6>Memory: 56636k/65536k available (1925k kernel code, 8840k reserved, 575k
data, 2716k init, 0k highmem)
<4>Calibrating delay using timer specific routine.. 1000.32 BogoMIPS
(lpj=1000322)
<4> available.
```

```
<4>Checking for the multiply/shift bug... no.  
<4>Checking for the daddi bug... no.  
<4>Checking for the daddiu bug... no.  
<5>detected lzma initramfs  
<5>initramfs: LZMA lc=3,lp=0,pb=2,dictSize=8388608,origSize=15217664  
<5>LZMA initramfs
```

Related Commands

Command	Description
tar	This command creates archive files in UNIX tar file format.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show ap debug crypto

```
show ap debug crypto
  ap-name <ap-name>
  detail {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
  history {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows the debug crypto logs for an AP.

Parameter	Description
ap-name <ap-name>	Shows debug crypto logs for the specified AP name.
detail	Shows detailed debug crypto logs for: <ul style="list-style-type: none">■ ap-name■ ip-addr■ ip6-addr
history	Shows historical debug crypto logs for: <ul style="list-style-type: none">■ ap-name■ ip-addr■ ip6-addr
ip-addr <ip-addr>	Shows debug crypto logs for the specified IP address of an AP.
ip6-addr <ip6-addr>	Shows debug crypto logs for the specified IPv6 address of an AP.

Example

The example shows the AP debug crypto logs of an AP named **MyAP**:

```
(host) [mynode] #show ap debug crypto ap-name MyAP

2014-01-07 14:48:43 ESP: spi[93477900] 10:15:64:104 << 10:15:66:151
2014-01-07 14:48:43 ESP: spi[ca0db300] 10:15:66:151 << 10:15:64:104
2014-01-07 15:19:34 SEND: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-07 15:19:34 RECV: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-07 15:19:39 SEND: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG:
INFORMATIONAL
2014-01-07 15:19:39 RECV: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG:
INFORMATIONAL
```

```

2014-01-07 18:00:49 RECV: 090cbf2a1ff1c433 : a496e13623118522 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-07 21:33:02 RECV: 090cbf2a1ff1c433 : a496e13623118522 , np=46, EXHG:
INFORMATIONAL
2014-01-07 22:49:00 SEND: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-07 22:49:00 RECV: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-07 22:49:00 ESP: spi[d774af00] 10:15:64:104 << 10:15:66:151
2014-01-07 22:49:00 ESP: spi[49799700] 10:15:66:151 << 10:15:64:104
2014-01-08 00:25:05 SEND: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-08 00:25:05 RECV: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG:
CREATE_CHILD_SA
2014-01-08 00:25:05 ESP: spi[83c32c00] 10:15:64:104 << 10:15:66:151
2014-01-08 00:25:05 ESP: spi[072a9200] 10:15:66:151 << 10:15:64:104

```

Related Commands

Command	Description
crypto-local isakmp allow-via-subnet-routes	Use this command to push subnet routes to the Mobility Conductor and managed device.
crypto-local isakmp ca-certificate	Use this command to assign the Certificate Authority (CA) certificate used to authenticate VPN clients.
crypto-local isakmp certificate-group	Use this command to assign a certificate group so you can access multiple types of certificates on the same managed device.
crypto-local isakmp disable-aggressive-mode	Use this command to disable the IKEv1 aggressive mode.
crypto-local isakmp dpd	Use this command to configure IKE Dead Peer Detection (DPD) on the managed device.
crypto-local isakmp key	Use this command to configure the IKE preshared key on the managed device for site-to-site VPN.
crypto-local isakmp server-certificate	Use this command to assign the server certificate used to authenticate the managed device for VPN clients.
crypto-local isakmp xauth	Use this command to enable the IKE XAuth for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug datapath

```
show ap debug datapath {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show datapath tunnel parameters of an AP or AP group.

Parameter	Description
ap-group <ap-group>	Shows data path information for a specific AP group.
ap-name <ap-name>	Shows data path information for an AP with a specific name.
bssid <bssid>	Shows data path information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows data path information for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	Shows data path information for an AP with a specific IPv6 address by entering an IP address in the dotted-decimal format.

Example

The output of the following command shows datapath tunnel parameters for an AP with the IP address 192.0.2.32.

```
(host) #show ap debug datapath ip-addr 192.0.2.32

Datapath Parameters Table
-----
essid   encr-alg      client-vlan-id  tunnel-id  gre-type  deny-bcast  num-clients
-----
-----
guest   Open          63              0x10f6    0x8300    disable     0
voip    WPA2 8021X AES 66              0x1103    0x8310    disable     7
corp    WPA2 PSK AES  66              0x10f1    0x8320    disable     0
guest   Open          63              0x10f7    0x8200    disable     1
wpa2    WPA2 8021X AES 65              0x10be    0x8210    enable      15
```

The output of this command includes the following information:

Column	Description
ESSID	The ESSID is a unique name that identifies a wireless network
encr-alg	Encryption algorithm used by the network
client-vlan-id	ID of the network VLAN
tunnel-id	Identification number of the AP's tunnel.
gre-type	GRE tunnel type.
deny-bcast	If enabled , the AP will respond to broadcast probe requests. If disabled , the AP will not respond to these requests.
num-clients	Number of clients currently using the network.

The output of the following command shows datapath tunnel parameters for an AP with the IPv6 address 11:12:11:11::2.

```
(host) #show ap debug datapath ip6-addr 11:12:11:11::2
Datapath Parameters Table
-----
essid          encr-alg      client-vlan-id  tunnel-id  gre-type
deny-bcast    num-clients
-----
-----
i-platform-mobility WPA2 PSK AES 10          0x1000b    0x8300
disable        0
i-platform-mobility WPA2 PSK AES 10          0x1000a    0x8200
disable        1
```

Related Commands

Command	Description
datapath	This command configures datapath options.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug dot11r efficiency

```
show ap debug dot11r efficiency <client-mac>
```

Description

This command displays all the r1 keys that are stored in an AP and the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming.

Parameter	Description
efficiency <client-mac>	Shows the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming for the specified client MAC address.

Examples

Use this command to view all the r1 keys that are stored in an AP.

```
(host) #show ap debug dot11r efficiency
Fast Roaming R1 Key Efficiency
-----
Client MAC          Hit (%)  Miss (%)
-----
00:50:43:21:01:b8  0 (0%)  0 (0%)
```

Related Commands

Command	Description
ap debug dot 11r remove-key	This command removes the r1 key from an AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug dot11r state

```
show ap debug dot11r state [ap-name <ap-name> | ip-addr <ip-addr>]
```

Description

This command displays all the r1 keys that are stored in an AP.

Parameter	Description
ap-name <ap-name>	Shows debugging information for a specific AP.
ip-addr <ip-addr>	Shows debugging information for an AP with a specific IP address by entering its IP address in the dotted-decimal format.

Examples

Use this command to view all the r1 keys that are stored in an AP. You can filter the output based on the AP name or IP address.

```
(host) #show ap debug dot11r state ap-name MAcage-105-GL

Stored R1 Keys
-----
Station MAC           Mobility Domain ID  Validity Duration  R1 Key
-----
00:50:43:21:01:b8    1                  3568                (32): 94 ff 18 0a
5f 47 8b 3e 95 2b
93 31 bd 44 58 fe fe 6a ad aa 1d d7 29 94 fb 5b 7c 15 76 66 d2 1f
```

Related Commands

Command	Description
ap debug dot 11r remove-key	This command removes the r1 key from an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on managed devices.

show ap debug driver-log

```
show ap debug driver-log {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip-addr>}
```

Description

This command shows an AP's driver logs. Use this command to review configuration changes made since the AP was last reset.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
bssid <bssid>	Shows log information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip-addr>	Shows log information for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.

Example

The following example shows an AP's driver logs:

```
(host) #show ap debug driver-log ap-name AP_205_26
rx fifo 0 overflows!
[2145812.982000] w11: 1 rx fifo 0 overflows!
[2145843.042000] w11: 8 rx fifo 0 overflows!
[2145860.478000] w11: 3 rx fifo 0 overflows!
[2145895.370000] stats > 100: ccastats_us: 52191, acc->statss_ms: 38
[2145903.172000] w11: 1 rx fifo 0 overflows!
[2145920.496000] w11: 1 rx fifo 0 overflows!
[2145933.232000] w11: 1 rx fifo 0 overflows!
[2145963.292000] w11: 2 rx fifo 0 overflows!
[2145980.522000] w11: 1 rx fifo 0 overflows!
[2145993.352000] w11: 1 rx fifo 0 overflows!
[2146023.412000] w11: 1 rx fifo 0 overflows!
[2146040.548000] w11: 3 rx fifo 0 overflows!
[2146053.472000] w11: 1 rx fifo 0 overflows!
[2146083.534000] w11: 3 rx fifo 0 overflows!
[2146100.576000] w11: 1 rx fifo 0 overflows!
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug esl-status

```
show ap debug esl-status {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows the ESL status of an AP. This command shows the values for ESL Server, ESL Channel, ESL Radio, Configuration Status, and the ESL Dongle ID of an AP.

Parameter	Description
ap-name <ap-name>	The name of the AP.
ip-addr <ip-addr>	The IP address of the AP.
ip6-addr <ip6-addr>	The IPv6 address of the AP.

Examples

The following example shows the ESL status of an AP:

```
(Host) *[mynode] #show ap debug esl-status ap-name AP32x_03
ESL Status
-----
Item                Value
----                -
ESL Server          0.0.0.0
ESL Channel         N/A
ESL Radio Coexistence Enabled
CONFIG State       INITIALIZED
ESL Dongle ID      N/A
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
AP-303H, 300 Series access points, 310 Series access points, 320 Series access points, 330 Series access points, 340 Series access points, and 510 Series access points	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug gre-tun-stats

```
show ap debug gre-tun-stats {ap-name <ap-name>| bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows GRE tunnel packet statistics of an AP.

Parameter	Description
ap-name <ap-name>	Shows GRE tunnel packets information for an AP.
bssid <bssid>	Shows GRE tunnel packets information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows GRE tunnel packets information for an AP with a specified IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows GRE tunnel packets information for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.

Example

The output of this command shows GRE tunnel packets information for an AP named AP325.

```
(host) #show ap debug gre-tun-stats ap-name AP325
GRE HBT Tunnel Stats
-----
AP IP      Controller IP  Sent Count  HBT Tx Seqnum  Idle (secs)  Rcvd Count
HBT Rx Seqnum
-----
-----
1.1.1.11   10.15.91.8    864681      12697          0            864636
12697

Idle (secs)
-----
0

GRE Tunnel Packet Stats
-----
MAC          BSSID          Tun Input  In IP Frags  To WLAN  Idle (secs)
Rate pps    From WLAN
-----
-----
C4:85:08:A2:15:2F  4F:4E:B0  54048      0            54048    60
5/          143339
```

```

00:26:C6:52:6B:7C 4F:4E:B0 31712 0 31712 120
2/ 69115
00:21:6A:B9:5F:34 4F:4E:B0 29628 3 29628 60
0/ 64985
FF:FF:FF:FF:FF:FF 4F:4E:B0 259841 0 259841 60
2/ 0
01:00:5E:00:01:74 4F:4E:B0 221714 6 221714 0
1/ 0
01:00:0C:CC:CC:CD 4F:4E:B0 443906 0 443906 0
0/ 0
01:00:5E:00:00:FC 4F:4E:B0 191310 0 191310 60
1/ 0

```

Tun	Output	Out IP	Frag	Idle (secs)	Rate pps
143339	143339	143339	0	0/	
69115	69115	69115	60	1/	
64985	64985	64985	60	1/	
0	0	0	0	0/	
0	0	0	0	0/	
0	0	0	0	0/	
0	0	0	0	0/	

NSS state

*** GRE offload feature is disabled (RAP) ***

NSS GRE Tunnel Stats

NSS IPv4 Node stats

ipv4 stats start:

common node stats:

rx_packets = 7119875

rx_bytes = 1547705849

rx_dropped = 0

tx_packets = 0

tx_bytes = 0

ipv4 node stats:

rx_pkts = 0

rx_bytes = 0

tx_pkts = 0

tx_bytes = 0

create_requests = 0

create_collisions = 0

create_invalid_interface = 0

destroy_requests = 0

destroy_misses = 0

hash_hits = 0

hash_reorders = 0

flushes = 0

evictions = 0

fragmentations = 0

mc_create_requests = 0

mc_update_requests = 0

mc_create_invalid_interface = 0

```

mc_destroy_requests = 0
mc_destroy_misses = 0
mc_flushes = 0
ipv4 exception stats:
IPV4_ICMP_HEADER_INCOMPLETE = 0
IPV4_ICMP_UNHANDLED_TYPE = 1743
.
.
.

```



The command output shows information only applicable for the specified AP. The output of the previous command is only a representative information of the likely output.

The output parameters in the command output (NSS State) are explained in the following table:

Column	Description
NSS LAG	Corresponds to the AP lag. This means that link aggregation is enabled on the Ethernet ports in NSS. This is only for the IP acceleration rule, so that NSS can expect packets coming in on both ports to match an acceleration rule. It is not necessarily for LACP. It is applicable for active-standby as well.
NSS Jumbo	Meant for the AP ports. This corresponds to the NSS phy layer setting to receive jumbo (9 KB) frames.
LMS GRE redi	Indicates GRE tunnel in NSS. In the output, the if_num value (for example, if_num 24) is the NSS interface number for a specific GRE tunnel.
LMS GRE rule	Refers to the IP-GRE acceleration rule for client traffic from and to the controller.
Standby GRE redir	Same as the LMS GRE redir, but corresponds to that of the standby controller.
Standby GRE rule	Same as the LMS GRE rule, but corresponds to that for the standby controller.
<p>NOTE: NSS refers to the network subsystem. It is a flow acceleration chipset from Qualcomm used in AP-315, and AP-325 access points. The hardware has Ethernet, IP, and GRE flow acceleration modules, IP fragmentation/reassembly, IPsec encap/decap. NSS also has the corresponding driver software. Most of these functions were performed by the software in previous AP models.</p>	

Related Commands

Command	Description
firewall	This command configures global firewall options on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap debug gsm-counters

```
show ap debug gsm-counters
  verbose
```

Description

Displays the GSM counters of an AP or AP group.

Parameter	Description
verbose	Shows the event statistics in a tabular format.

Example

The output of the following command shows gsm counters of an AP:

```
(host) (config) #show ap debug gsm-counters verbose
STM GSM Counters
-----
Name                                     Value
----                                     -
AP Publish Events                       15
AP Delete Events                         3
Radio Publish Events                    9548
Radio Delete Events                     0
BSS Publish Events                      6
Responses to BSS Rcvd                   6
BSS Delete Events                       0
STA Publish Events                      0
STA Delete Events                       0
WIRED_AP Publish Events                  0
Responses to WIRED_AP Rcvd              0
WIRED_AP Delete Events                  0
MAC-User Publish Notifications           0
MAC-User Notify Events                  0
MAC-User Responses Sent                  0
BSS Response time histogram [1...128] seconds in powers of 2 4 2 0 0 0 0 0
0
STA Response time histogram [1...128] seconds in powers of 2 0 0 0 0 0 0 0
0
STA Delete Reason                         Count
-----
```

Related Commands

Command	Description
show lc cluster	This command displays information related to vlan, membership, profile, heartbeat, and so on for a cluster.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug hotspot statistics bssid

```
show ap debug hotspot statistics bssid <bssid_string>
```

Description

This command shows the statistics of ANQP/H2QP information.

Parameter	Description
bssid <bssid_string>	Shows statistics of ANQP/H2QP information for the specified BSSID.

Example

The following example shows the statistics of ANQP/H2QP information for the BSSID 00:1a:1e:aa:bb:cc:

```
(host) [mynode] #show ap debug hotspot statistics bssid 00:1a:1e:aa:bb:cc
```

Related Commands

Command	Description
aaa authentication stateful-dot1x	This command configures a RADIUS server.
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an ANQP information element in a GAS query response.
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an ANQP information element in a GAS query response.

Command	Description
<u>wlan hotspot anqp-nai-realm-profile</u>	This command defines a Network Access Identifier realm whose information can be sent as an ANQP information element in a GAS query response
<u>wlan hotspot anqp-nwk-auth-profile</u>	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.
<u>wlan hotspot anqp-roam-cons-profile</u>	This command configures the Roaming Consortium OI information to be sent in an ANQP information element in a GAS query response
<u>wlan hotspot anqp-venue-name-profile</u>	This command defines venue information be sent in an ANQP information element in a GAS query response.
<u>wlan hotspot h2qp-conn-capability-profile</u>	Defines a H2QP profile that advertises hotspot protocol and port capabilities.
<u>wlan hotspot h2qp-op-cl-profile</u>	Defines a H2QP profile that defines the Operating Class to be sent in the ANQP IE.
<u>wlan hotspot h2qp-operator-friendly-name-profile</u>	Defines a H2QP operator-friendly name profile.
<u>wlan hotspot h2qp-wan-metrics-profile</u>	Creates a H2QP profile that specifies the hotspot WAN status and link metrics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug iot-sniffer

```
show ap debug iot sniffer {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip-addr>}  
radio {all|<radio-mac-addr>}
```

Description

This command shows IoT sniffer information on the AP.

Parameter	Description
ap-name <ap-name>	Shows IoT information for an AP with a specific name.
ip-addr <ip-addr>	Shows IoT information for an AP with a specific IP address.
ip6-addr <ip-addr>	Shows IoT information for an AP with a specific IPv6 address.
radio	Shows IoT information of the radio in an AP
all	Shows IoT information of all radios in an AP.
<radio-mac-addr>	Shows IoT information of a specific radio in an AP.

Example

The following example displays an AP's ipc forwarding statistics.

```
(host) [mynode] #show ap debug iot-sniffer ap-name AP-215 radio all
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug ipc forwarding-statistics

```
show ap debug ipc forwarding-statistics {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip-addr>}
```

Description

This command shows an AP's ipc forwarding statistics. Use this command to review configuration changes made since the AP was last reset.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip-addr>	Shows log information for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.

Example

The following example displays an AP's ipc forwarding statistics.

```
(host) #show ap debug ipc forwarding-statistics ap-name AP_205_26
IPC Forwarding Statistics for AP "Usha_AP_205_26" (Fri Nov 6 05:11:10 2020)
-----
IP          Source          Destination          Dir
Forward
-----
          ed Packets  Forwarded Bytes  Dropped Packets  Dropped Bytes
--          -
-----
10.17.24.22 AP STM Low Priority          AirWave Mgmt Server  Out  5
          840          0          0
10.17.24.22 SAPM          SAPM Client          In
8967
          1258761          0          0
10.17.24.22 SAPM Client          SAPM          Out
116521
          20557043          0          0
```

10.17.24.22 73162	WMS			AM		In
10.17.24.22 565542	AM	21442393	0	Message Handler	0	Out
10.17.24.22 127907	AM	1988592961	0	ARM Process	0	Out
10.17.24.22 167967	AM	192224651	0	STM Low Priority	0	Out
10.17.24.22 18718	AM	602448528	0	AMAPI SNMP trap client	0	Out
10.17.24.22 43664	AM	2784470	0	AirWave Mgmt Server	0	Out
10.17.24.22 113514	ARM Process	43749552	0	AM	0	In
10.17.24.22 35777	USB Dongle Management Daemon	11507252	0	SAPM	0	Out
		3327261	0		0	

Related Commands

Command	Description
show ipc statistics	This command displays the Inter Process Communication (IPC) statistics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug lacp

```
show ap debug lacp {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr<ip6-addr>}
```

Description

This command shows the number of GRE packets sent and received on the two Ethernet ports. Use this command to know if LACP is active on an AP from the number of GRE packets sent and received on the two Ethernet ports. If a GRE striping IP address is configured in the **ap-lacp-striping-ap** profile, the output of this command displays the GRE striping IP address.

Parameter	Description
ap-name <ap-name>	Shows LACP information for an AP with a specific name.
bssid <bssid>	Shows LACP information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows LACP information for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows LACP information for an AP with a specific IPv6 address.

Example 1

The following example displays that the wireless GRE packets are being sent and received on different wired ports of the AP for the 5GHz and 2.4GHz bands, and is only applicable to 220 Series and 270 Series. It also shows that the interfaces eth0 and eth1 are part of the link aggregation group (LAG):

```
show ap debug lacp ap-name 3ap225

AP LACP GRE Striping IP: 10.65.30.50
AP LACP Status
-----
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----
Up           slow       2          17         2           00:0b:86:61:7a:58
Slave/Member Interface Status
-----
Slave/Member I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link
Fail Count
-----
---
eth0                  6c:f3:7f:c6:72:82  Up           Yes            0
eth1                  6c:f3:7f:c6:72:83  Up           Yes            1
```

GRE Radio Traffic Received on Enet Ports

```
-----  
Radio Num  Enet 0 Rx Count  Enet 1 Rx Count  
-----  
0          5048          0  
1          0            23
```

Traffic Sent on Enet Ports

```
-----  
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count  
-----  
0          65            3466  
1          64            0  
non-wifi   2            50
```

The following example is only applicable to 320 Series:

#show ap debug lacp ap-name ap325 verbose

AP LACP GRE Striping IP: 10.3.44.34

AP LACP Status

```
-----  
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC  
-----  
Up          slow       2          17         4           00:1a:1e:0f:b4:80
```

Slave/Member Interface Status

```
-----  
Slave/Member I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link  
Fail Count
```

```
-----  
---  
eth0          ac:a3:1e:cd:35:ce  Up           Yes           1  
eth1          ac:a3:1e:cd:35:cf  Up           Yes           1
```

GRE Traffic Received on Enet Ports

```
-----  
Radio Num  Enet 0 Rx Count  Enet 1 Rx Count  
-----  
0          23785          22083  
1          0            0  
non-wifi   15684          3
```

Traffic Sent on Enet Ports

```
-----  
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count  
-----  
0          8166          307  
1          0            0  
non-wifi   32326          7
```

Link Aggregation destination list

```
-----  
[ 0] 00:1A:1E:01:4F:28 Tx: 6008  
[ 1] 24:77:03:F4:82:B4 Tx: 28  
[ 2] 78:31:C1:BC:D6:12 Tx: 26  
[ 3] F0:1F:AF:69:51:9E Tx: 229
```

Total: 4

Odd numbered entries use striping GRE tunnel.

Total tunnel mode AMSDU Tx: 99

Link Aggregation station packet re-ordering statistics

```
3C:A9:F4:24:B2:54: exp-seq 21; eap 0 zero 0; rx 20 tx 20 drop 0 max_hold 0
skip 0 old-seq 0(last-seq# 0); window: resets 0 pkts 0; Timer: start 0 stop
0 run 0 more 0
78:31:C1:BC:D6:12: exp-seq 223; eap 0 zero 0; rx 222 tx 222 drop 0 max_hold
0 skip 0 old-seq 0(last-seq# 0); window: resets 0 pkts 0; Timer: start 0
stop 0 run 0 more 0
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>slave</code> have been replaced with <code>member</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug lldp

```
show ap debug lldp
```

Description

This command shows an AP's debug log.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
bssid <bssid>	Shows log information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering an IP address in the dotted-decimal format.

An AP's log files show configuration changes since the AP was last reset.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug lldp counters

```
show ap debug lldp counters {ap-name <ap-name>} {ip-addr <ip-addr>} {ip6-addr <ip6-addr>} [interface <port-string>]
```

Description

This command shows LLDP statistics of an AP.

Parameter	Description
ap-name <ap-name>	Shows LLDP statistics of an AP for specified AP name.
ip-addr <ip-addr>	Shows LLDP statistics of an AP for specified IP address.
ip6-addr <ip6-addr>	Shows LLDP statistics of an AP for specified IPv6 address.
interface <port-string>	Shows LLDP statistics for specified interface of an AP.

Example

The following example shows radio scanning of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp counters ap-name ap-205

LLDP Counters
-----
Interface  Received  Unknown TLVs  Malformed  Overflow  Transmitted
-----
bond0      49937     0              0           0         49914
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug lldp neighbors

```
show ap debug lldp neighbors {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>} [interface <port-string> [detail]]
```

Description

This command shows LLDP peer information of an AP.

Parameter	Description
ap-name <ap-name>	Shows LLDP peer information of an AP for specified AP name.
ip-addr <ip-addr>	Shows LLDP peer information of an AP for specified IP address.
ip6-addr <ip6-addr>	Shows LLDP peer information of an AP for specified IPv6 address.
interface <port-string> [detail]	Shows LLDP peer information for specified interface of an AP. Detail parameter shows additional LLDP peer information.

Example

The following example shows LLDP peer information of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp neighbors ap-name ap-205

Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-----
Interface  Neighbor ID          Capabilities  Remote Interface  Expiry-Time
(SeCs)    -----
-----
bond0      00:0b:86:96:fe:f7   B:R          GE0/0/2           91

Number of neighbors: 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug lldp state

```
show ap debug lldp state {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>} [interface <port-string>]
```

Description

This command shows LLDP state of an AP.

Parameter	Description
ap-name <ap-name>	Shows LLDP state of an AP for specified AP name.
ip-addr <ip-addr>	Shows LLDP state of an AP for specified IP address.
ip6-addr <ip6-addr>	Shows LLDP state of an AP for specified IPv6 address.
interface <port-string>	Shows LLDP state for specified interface of an AP.

Example

The following example shows LLDP state of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp state ap-name ap-205

LLDP Interface Information
-----
Interface  LLDP TX  LLDP RX  LLDP-MED  TX interval  Hold Timer
-----
bond0      Enabled  Enabled  Disabled  30           120
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug log

```
show ap debug log {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows an AP's debug log. An AP's log files show configuration changes since the AP was last reset.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
bssid <bssid>	Shows log information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	Shows log information for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug log-config

```
show ap debug log-config {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows AP log configuration.

Parameter	Description
ap-name <ap-name>	Shows AP log configuration for specified AP name.
ip-addr <ip-addr>	Shows AP log configuration for specified IP address.
ip6-addr <ip6-addr>	Shows AP log configuration for specified IPv6 address.

Example

The following example shows an AP named ap-205 is not registered with managed device:

```
(host) [mynode] #show ap debug log-config ap-name ap-205
AP is not registered with this switch
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug multizone

```
show ap debug multizone
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows the MultiZone configured for an AP.

Parameter	Description
ap-name <ap-name>	Name of AP.
ip-addr <ip-addr>	IP Address of AP.
ip6-addr <ip6-addr>	IPv6 address of AP.

Example

The following example shows the MultiZone configured for a particular AP:

```
(host) [mynode] (config) #show ap debug multizone ap-name RFCage05_AP214_2_
C_6_7031

Multizone Table
-----
Zone  Configured IP      Serving IP          Max Vaps Allowed  Nodes  Flags
----  -
0     10.16.84.10        10.16.84.10        13 (0~12)         1      2
1     2008::abc:90:90::4 2008::abc:90:90::4 3 (0-2)            1      V
Flags: C = Cluster; L = Limited nodes; N = Nodes in other zones; 2 = Using
IKE version 2; M = Image mismatch; V = IP version mismatch
Number of datazones:1
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the <code>show ap debug multizone</code> command was modified to include V flags that indicate the IP version mismatch between primary zone and data zone configuration.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode in managed devices.

show ap debug mu-status

```
show ap debug mu-status
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows detailed MU status of the clients associated with an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	SA status data for an AP with a specific name.
bssid <bssid>	SA status data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	SA status data for an AP with a specific IP address by entering an IP address in the dotted-decimal format.
ip6-addr <ip6-addr>	SA status data for an AP with a specific IPv6 address by entering an IPv6 address in the dotted-decimal format.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug openflow

```
show ap debug openflow
  flows {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
  state {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} detail
```

Description

This command shows the OpenFlow protocol.

Parameter	Description
<code>flows {ap-name <ap-name> ip-addr <ip-addr> ip6-addr <ip6-addr>}</code>	Shows OpenFlow protocol flows filtered by specified AP name, IP address of an AP, or IPv6 address of an IP.
<code>state {ap-name <ap-name> ip-addr <ip-addr> ip6-addr <ip6-addr>} detail</code>	Shows basic or detailed OpenFlow protocol state filtered by specified AP name, IP address of an AP, or IPv6 address of an AP.

Example

Access the CLI and use the following command to show basic OpenFlow protocol state of AP **test**:

```
(host) [mynode] #show ap debug openflow state ap-name test

Controller IP: 0.0.0.0, port:0, State: Init, Last Up:Thu Jan  1 05:30:00
1970, Last down:Thu Jan  1 05:30:00 1970
Openflow Interface List
  IF MAC:9c:1c:12:c0:95:c8, port_no:8453, name:bond0, oflow_index:0
OpenFlow MAC Bridge List
OpenFlow Dynamic Tunnel List
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug port status

```
show ap debug port status {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows the status of the AP's wired ports.

Parameter	Description
ap-name <ap-name>	Name of the AP.
bssid <bssid>	BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.

Examples

The output of the command displays the wired port status of an AP named **LocalAP1**. In this example, the output is divided into multiple sections to fit better on the pages of this document. In the actual CLI, it appears in a single long table.

```
(host) [mynode] #show ap debug port status ap-name LocalAP1

AP "LocalAP1" Port Status
-----
Port  MAC                Type  Forward Mode  Admin    Oper   Speed
Duplex 802.3az 802.3bz  PoE
-----
-
0      00:1a:1e:10:05:1a  GE    N/A           enabled  up     1 Gb/s  full
N/A    N/A          N/A
1      00:1a:1e:10:05:1b  FE    tunnel        enabled  up     100 Mb/s full
N/A    N/A          N/A
2      00:1a:1e:10:05:1c  FE    tunnel        enabled  down   N/A     N/A
N/A    N/A          N/A
3      00:1a:1e:10:05:1d  FE    N/A           disabled down   N/A     N/A
N/A    N/A          N/A

STP          TX-Packets  TX-Bytes  RX-Packets  RX-Bytes
---          -
N/A          23697       3338307   27449       8471871
Forwarding   12185       6593226   18436       1758272
Disabled     0           0         0           0
Off          0           0         0           0
```


Command History

Release	Modification
ArubaOS 8.3.0.0	The output of the <code>show ap debug port status</code> command was modified to add a new column 802.3bz to show the 802.3bz state of the wired port.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug power-table

```
show ap debug power-table {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}  
{radio <radio id>}
```

Description

Displays the following information for a specific radio:

- Power limit table based on regulatory powers, user configured power, and override powers.
- Board limit table.
- A combination of all the above fields to calculate the actual transmit power of the packets.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows power table for an AP with a specific name.
ip-addr <ip-addr>	Shows power table for an AP with a specific IP address.
ip6-addr <ip6-addr>	Shows power table for an AP with a specific IPv6 address.
radio <radio id>	Radio ID (0, 1, or 2).

Examples

The output of this command displays power table from an AP-225.

```
(host) [mynode] #show ap debug power-table ap-name AP-225 radio 0
```

Command History

Release	Modification
ArubaOS 8.10.0.0	The command output was modified to include <code>Flash EIRP Limit</code> parameter for 6 GHz bands.
ArubaOS 8.6.0.0	Radio ID 2 was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug radar-logs

```
show ap debug radar-logs
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows the latest four RADAR event logs from the AP. This command is useful for debugging false radar detection related issues.



This command is applicable for APs running the Broadcom chipset.

Parameter	Description
ap-name <ap-name>	Displays RADAR logs for an AP with a specific name.
ip-addr <ip-addr>	Displays RADAR logs for an AP with a specific IP address.
ip6-addr <ip6-addr>	Displays RADAR logs for an AP with a specific IPv6 address.

Example

The output of this command displays RADAR logs from an AP-225.

```
(host) #show ap debug radar-logs ap-name AP-225

The latest 4 radar event logs
Radar logs:

Pruned Intv:
3220-0
3220-1
3220-2
3220-3
3220-4
3220-5
3220-6
3220-7
3220-8
3220-9
3220-10

Pruned PW:
50-0
50-1
50-2
```

50-3
50-4
50-5
50-6
50-7
50-8
50-9
50-10

Nepochs=1 len=27 epoch_#=1; det_idx=0 pw_delta=0 min_pw=50 max_pw=50
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_ pulses=5. Time from last detection = 19, = 0min 19sec, Time 244

+++++

Radar logs:

Pruned Intv:

4140-0
4140-1
4140-2
4140-3
4140-4
4140-5
4140-6
4140-7
4140-8
4140-9
4140-10

Pruned PW:

19-0
18-1
18-2
19-3
19-4
18-5
19-6
18-7
18-8
18-9
18-10

Nepochs=1 len=30 epoch_#=1; det_idx=0 pw_delta=1 min_pw=18 max_pw=19
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_ pulses=9. Time from last detection = 3, = 0min 3sec, Time 247

+++++

Radar logs:

Pruned Intv:

4200-0
4200-1
4200-2
4200-3
4200-4
4200-5

4200-6
4200-7
4200-8
4200-9
4200-10

Pruned PW:

17-0
18-1
17-2
16-3
17-4
17-5
17-6
17-7
17-8
17-9
17-10

Nepochs=1 len=30 epoch_#=1; det_idx=0 pw_delta=2 min_pw=16 max_pw=18
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_ pulses=9. Time from last detection = 3, = 0min 3sec, Time 250
++++
++++
Radar logs:
Valid LP: KIntv=151077 Ksalintv=27820 PW=1557 FM=255 pulse#=0 pw2=0 pw_dif=0 pw_tol=8 fm2=0 fm_dif=0 fm_tol=0
nLP=1 nSKIP=0 skipped_salvate=0 pw_fm_matched=0 #non-single=0 skip_tot=0 csect_single=1
Valid LP: KIntv=23 Ksalintv=23 PW=1558 FM=255 pulse#=1 pw2=1557 pw_dif=1 pw_tol=8 fm2=255 fm_dif=0 fm_tol=127
nLP=2 nSKIP=0 skipped_salvate=0 pw_fm_matched=1 #non-single=1 skip_tot=0 csect_single=0
Valid LP: KIntv=36 Ksalintv=36 PW=1557 FM=255 pulse#=2 pw2=1558 pw_dif=1 pw_tol=8 fm2=255 fm_dif=0 fm_tol=127
nLP=3 nSKIP=0 skipped_salvate=0 pw_fm_matched=2 #non-single=2 skip_tot=0 csect_single=0
Skipped LP: nLP=3 nSKIP=1 KIntv=59 Ksalintv=59 PW=1557 FM=255 Type=4 pulse#=3 skip_tot=1 csect_single=0
Valid LP: KIntv=35680 Ksalintv=35740 PW=1904 FM=255 pulse#=0 pw2=0 pw_dif=0 pw_tol=8 fm2=0 fm_dif=0 fm_tol=0
nLP=4 nSKIP=0 skipped_salvate=0 pw_fm_matched=2 #non-single=2 skip_tot=1 csect_single=1
Valid LP: KIntv=25 Ksalintv=25 PW=1904 FM=255 pulse#=1 pw2=1904 pw_dif=0 pw_tol=8 fm2=255 fm_dif=0 fm_tol=127
nLP=5 nSKIP=0 skipped_salvate=0 pw_fm_matched=3 #non-single=3 skip_tot=1 csect_single=0
Valid LP: KIntv=28 Ksalintv=28 PW=1904 FM=255 pulse#=2 pw2=1904 pw_dif=0 pw_tol=8 fm2=255 fm_dif=0 fm_tol=127
nLP=6 nSKIP=0 skipped_salvate=0 pw_fm_matched=4 #non-single=4 skip_tot=1 csect_single=0
FCC-5 Radar Detection. Time from last detection = 17, = 0min 17sec, Time 454
++++
++++

Parameter	Description
Pruned Intv	Displays the filtered and pre-processed RADAR pulse interval.
Pruned PW	Displays the filtered and pre-processed RADAR pulse width.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug radio-diag-log status

```
show ap debug radio-diag-log <status>
```

Description

This command displays the current diagnostic logging status of an AP.

Parameter	Description
status	Displays the current diagnostic logging status.

Example

The following command displays the output after the `ap debug radio-diag-log start` command is executed:

```
(host) [mynode] #show ap debug radio-diag-log status ap-name ap555
Status: Started. radio-diag-log is in progress
Log size: 3145728 bytes
grep pattern: -e WMI -e WAL
Error: None
Dump server: 10.100.225.27
Transfer mode: scp
```

Related Commands

Command	Description
ap debug radio-diag-log	This command collects WLAN firmware diagnostic logs to facilitate firmware debugging.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
AP-534, AP-535, AP-555 access points	Base operating system.	Enable mode on Mobility Conductor.

show ap debug radio-event-log status

```
show ap debug radio-event-log status {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show information about the radio event information captured in packet log files.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
ip-addr <ip-addr>	Shows log information for an AP with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows log information for an AP with a specific IPv6 address by entering its IPv6 address.

Example

```
Radio Event Logs
-----
Radio Index  Radio's Bssid      Radio's Band  Event Type  Log File Size
Status
-----
---
0           00:24:6c:bd:65:b0  80211a       N/A         N/A
start
1           00:24:6c:bd:65:a0  80211g       N/A         N/A
stop
```

The output of this command includes the following information:

Parameter	Description
radio Index	Index number of the AP radio (0 or 1).
Radio's BSSID	BSSID of the AP radio. This is typically the AP radio's MAC address.
Radio's Band	Band used by the AP radio.
Event Type	Type of events recorded. By default, all supported event types are recorded. <ul style="list-style-type: none">■ N/A: The default event type setting, which captures all

Parameter	Description
	<p>supported types of radio events.</p> <ul style="list-style-type: none"> ■ ani Adaptive Noise Immunity control events ■ rcfind: Transmission (Tx) control event ■ rcupdate: Transmission (Tx) rate update event ■ rx: Received (Rx) status register event ■ text: Text record event ■ tx: Transmission (Tx) control and Tx status register event
Log File Size	Size of the log file. A value of N/A indicates that the packet log feature uses the default log file size of 3145728 bytes (3MB).
Status	Shows if packet log capture was started or stopped on the AP radio.

Related Commands

Command	Description
ap debug radio-event-log	This command starts and stops packet log capture of radio events for debugging purposes, and sends a log file of the events to a dump server when logging stops.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug radio-info

```
show ap debug radio-info
  ap-name <ap-name> radio <radio id>
  ip-addr <ip-addr> radio <radio id>
  ip6-addr <ip6-addr> radio <radio id>
```

Description

This command shows the Wi-Fi radio debug logs from the AP driver.



This command is applicable for 200 Series, 210 Series, 220 Series, 270 Series, and 550 Series access points.

Parameter	Description
ap-name <ap-name>	Shows Wi-Fi radio debug logs for an AP with a specific name.
ip-addr <ip-addr>	Shows Wi-Fi radio debug logs for an AP with a specific IP address.
ip6-addr <ip6-addr>	Shows Wi-Fi radio debug logs for an AP with a specific IPv6 address.
radio <radio id>	Radio ID (0, 1, or 2)

Example

The output of this command displays the log information about Wi-Fi radio 0 for an AP-225:

```
(host) #show ap debug radio-info ap-name AP-225 radio 0

Radio Info Script
-----
aruba_dbg_radio_info_0 Start time: Fri Mar 27 14:33:21 IST 2015
-----
wifi0-drop-list:
_dma_rxreclaim(1633): 2520/2520 0/0
wlc_recvctl(44993): 3130421/3130421 0/0
wlc_dotxstatus(41101): 2502/2502 2502/2502
...
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Radio 2 radio ID was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug radio-registers

```
show ap debug radio-registers {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>} {radio 0|1|2}
```

Description

This command allows you to view radio register changes.

Parameter	Description
ap-name <ap-name>	Name of the AP for which you want to view register changes.
ip-addr <ip-addr>	IPv4 address of the AP for which you want to view register changes.
ip6-addr <ip6-addr>	IPv6 address of the AP for which you want to view register changes.
radio 0 1 2	Shows information for the specified radio on the AP.

This command displays radio register changes made under the supervision of Aruba technical support.

Command History

Release	Modification
ArubaOS 8.6.0.0	Radio 2 radio ID was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug radio-stats

```
show ap debug radio-stats {ap-name <ap-name>|ip-addr <ip-addr>} radio {0|1|2}
[advanced]
```

Description

This command shows aggregate radio debug statistics of an AP.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	IPv6 address of the Access Point.
radio {0 1 2}	Specify the ID number of the radio for which you want to view statistics.
advanced	Include this parameter to display additional radio statistics.

Example

The output of this command displays general statistics for the radio, as well as statistics for transmitted and received frames.

```
(host) #show ap debug radio-stats ap-name AP12 radio 1
RADIO Stats
-----
Parameter          Value
-----
-----
General Per-radio Statistics
Total Radio Resets 0
Resets Beacon Fail 0
TX Power Changes   5
Channel Changes    2
Radio Band Changes 0
Current Noise Floor 95
llg Protection     0
-----
Transmit specific Statistics
Frames Rcvd For TX 2452151
Tx Frames Dropped  1736429
Frames Transmitted 4247212
Tx EAPOL Frames    0
TX STBC Frames     0
TX LDPC Frames     0
Tx AGGR Good       0
```

```

Tx AGGR Unaggr                20
Tx Data Priority [BE]         20
Tx Data Frames 12 Mbps (Mon)  0
Tx Data Frames 24 Mbps (Mon)  0
Tx Data Frames 36 Mbps (Mon)  0
Tx Data Frames 54 Mbps (Mon)  0
Tx Data Frames 72 Mbps (Mon)  0
Tx Data Frames 108 Mbps (Mon) 0
Tx Data Frames 300 Mbps (Mon) 20
Tx Data Frames 450 Mbps (Mon) 0
Tx Data Frames 1300 Mbps (Mon) 0
Tx Data Frames 1300 Mbps+ (Mon) 0
Tx Data Bytes 12 Mbps (Mon)  0
Tx Data Bytes 24 Mbps (Mon)  0
Tx Data Bytes 36 Mbps (Mon)  0
Tx Data Bytes 54 Mbps (Mon)  0
Tx Data Bytes 72 Mbps (Mon)  0
Tx Data Bytes 108 Mbps (Mon)  0
Tx Data Bytes 300 Mbps (Mon) 4371
Tx Data Bytes 450 Mbps (Mon)  0
Tx Data Bytes 1300 Mbps (Mon)  0
Tx Data Bytes 1300 Mbps+ (Mon) 0
Tx 6 Mbps                      7
Tx HT 130 Mbps                 20
Tx WMM [BE]                   20
Tx UAPSD OverflowDrop         0
TX Timeouts                   0
Lost Carrier Events           0
Tx HT40 Hang Detected         0
Tx HT40 Hang Stuck            0
Tx HT40 Hang Possible         0
Tx HT40 Dfs IMM WAR           0
Tx HT40 Dfs HT20 WAR          0
Tx MAC/BB Hang Stuck          0
Tx Mgmt Bytes                  415
Tx Beacons Bytes              0
Tx Managment Frames Dropped    1
Tx AMSDU pkt count            0
Tx EAPOL Frames Rcvd          0
Tx EAPOL Frames Dropped       0
Tx Data Frames MCS 7          20
Tx Data Frames MCS             20
Tx Data Frames NSS2           20
Tx Data Frames Long-GI (FULL) 20
Tx Data Frames BW 20          20
-----
Rx Last SNR                    15
Rx Last SNR CTL0              15
Received Statistics

```

If you include the **advanced** option at the end of the `show ap debug radio-stats` command, the output of this command will include all the following parameters, as well as additional information for the SNR, frame counts, channel busy times, and data bytes for transmitted and received packets. If you omit the **advanced** option, the output will include less information, and the data will be displayed in a different order. The following table describes the output of this command when the **advanced** option is included.

Parameter	Description
Total Radio Resets	Total number of times the radio reset.
Resets Beacon Fail	Number of times the radio reset due to beacon failure.
BB check positives	Number of times the radio checked for a base-band hang condition
Resets BeacQ Stuck	An AP's radio typically sends a beacon every 100 milliseconds. If beacons are not sent at a regular interval or the radio experiences excessive noise, the beacon queue will reset. This parameter indicates the number of queue resets.
Resets Fatal Intr	Number of time the radio was reset because the AP hardware was unresponsive.
Resets RX Overrun	The number of radio resets due to Receive FIFO overruns.
Resets RF Gain	Number of radio resets due to gain changes.
Resets MTU Change	Number of times the radio reset due to a change in the Maximum Transmission Unit (MTU) value.
Resets TX Timeouts	Number of radio resets due to transmission timeouts (the radio doesn't transmit a signal within the required time frame.)
POE-Related Resets	If the radio power profile drops, an AP may not be able to support three transmit chains, and may drop to two chains only. This parameter displays the number of resets due to this type of power change.
External Reset	Number of times the AP has been reset because it was unplugged or its reset button was pressed.
PCI Fatal Intr Reset	Radio reset due to PCI fatal interrupt received from radio chip.
Chaimask Reset	Radio reset when new chain mask is configured.
TX stat Reset	Radio reset caused by inconsistent state of hardware transmit queue.
TX Power Changes	Number of times the radio's transmission power changed.
Channel Changes	Number of times the radio's channel changed.
Radio Band Changes	Number of time the radio's band changed.

Parameter	Description
Current Noise Floor	The residual background noise detected by an AP. Noise seen by an AP is reported as -dBm. Therefore, a noise floor of -100 dBm is smaller (lower) than a noise floor of -50 dBm. For most environments, the noise floor should be no greater than -80 dBm. Anything larger may indicate an interference problem which is drowning out good signals (data) in background noise.
Dummy NF pkts on home channel	Number of noise floor readings on the home channel.
Dummy NF pkts on scan channel	Number of noise floor readings on the scan channel.
Avail TX Buffers	An AP has a set number of buffers which it can use to buffer frames for non-responsive power save clients. The total number of buffer frames depends upon the AP model type.
11g Protection	This parameter shows whether 802.11g protection has been enabled or disabled.
Last TX Antenna	This parameter indicates whether the last frame transmitted was sent on antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Last RX Antenna	This parameter indicates whether the last frame received was via antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Scan Requests	Total number of scan requests received by the AP.
Scan Rejects	Total number of scan rejected by the AP.
Scan Rejects (Misc 1)	Number of scan rejects due to pending transmissions.
Load aware Scan Rejects	Load aware ARM preserves network resources during periods of high traffic by temporarily halting scanning if the load for the AP gets too high. The <code>load aware Scan Rejects</code> parameter shows the number of times the AP has rejected a scan because of the load aware scan feature.

Parameter	Description
PS aware Scan Rejects	If the ARM power-save aware scan feature is enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. The <code>ps aware Scan Rejects</code> parameter shows the number of times the AP has rejected a scan because of the power-save aware scan feature.
EAP Scan Rejects	If you enable the EAP-aware scanning feature in the AP's ARM profile, the AP will not attempt to scan a different channel if the Extensible Authentication Protocol over LAN (EAPOL) exchange is in progress with a client. This parameter shows the number of times the AP has rejected a scan because of the EAP aware scanning feature.
Voice aware Scan Rejects	If you enable the VoIP Aware Scan feature in the AP's ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This <code>Voice aware scan Rejects</code> parameter shows the number of times the AP has rejected a scan because of the Voip aware scan feature.
Video aware Scan Rejects	If you enable the Video Aware Scan feature in the AP's ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active video session. This <code>Video aware scan Rejects</code> parameter shows the number of times the AP has rejected a scan because of the Video aware scan feature.
UAPSD Scan Rejects	Number of times the scan was rejected due to UAPSD-related transmissions.
Post radar related scan Rejects	Number of times the scan was rejected due to recent radar detection.
CABQ traffic Scan Rejects	Number of times the scan was rejected due to pending multicast transmissions.
Radio Reset Scan Rejects	Number of times the scan was rejected due to a recent radio reset.
Queue Drain Scan Rejects	This legacy statistic has been deprecated, and will not increment.
Scan Success	Number of successful scans. To view scan details, use the command show ap arm scan-times .

Parameter	Description
Scan Deferred	Number of times the scan was deferred due to pending beacon transmissions on the home channel.
EIRP	The value of this parameter is the transmission power level (in dBm) + the antenna gain value.
MAX EIRP	The max EIRP depends on AP capability and the regulatory domain constraint for the channel of operation. For example, in the US, Channels 36-48 have max EIRP of 23dBm
Dummy<number>	For internal use only.
UAPSD Flush STA Wake	Number of times a client wakes from power-save mode and flushes the UAPSD queue.
UAPSD SP Set	The number of unique UAPSD Scheduled Period is started in response to UAPSD trigger frames.
UAPSD Dup Trig	The number of times duplicate UAPSD trigger frames are received (i.e., retried UAPSD triggers that were received by the AP more than once).
UAPSD Recv frame for TX	The number of frames received for transmission over the air interface using UAPSD
UAPSD Ageout Drain	The number of time UAPSD queue is drained (i.e. frames are dropped) due to ageout.
UAPSD TX proc comp	The number of UAPSD frames that were successfully transmitted
UAPSD SP In prog	The number of times a trigger frame was received while a Scheduled Period (SP) was already in progress based on an earlier trigger frame.
UAPSD QOS NULL TX	The number of times the AP had to respond with a QoS Null Data frame in response to a UAPSD trigger because AP did not have Data frame queued for that client
UAPSD TX HW Queued	The number of frames (Data and Null Data) that were transferred to the radio HW for transmission, in response to UAPSD triggers.
UAPSD SP Reset	The number of times the UAPSD Scheduled Period (SP) in progress is reset or canceled.
Tx Time perct @ beacon intvl	Percentage of time spent transmitting Wi-Fi frames since the last beacon.

Parameter	Description
Tx Frames Rcvd	Number of transmitted frames that were received.
Tx Bcast Frames Rcvd	Number of transmitted broadcast frames that were received.
Tx Frames Dropped	Number of transmitted frames that were dropped.
Tx Bcast Frames Dropped	Number of transmitted broadcast frames that were dropped.
Tx Frames Transmitted	Number of frames successfully transmitted.
Tx Bytes Rcvd	Number of transmitted bytes received.
Tx Bytes Transmitted	Number of transmitted bytes
Tx Time Frames Rcvd	Number of times transmitted frames were received.
Tx Time Frames Dropped	Number of times transmitted frames were dropped.
Tx Time Frames Transmitted	Number of times frames were transmitted.
Tx PS Unicast	Number of power save unicast frames
Tx DTIM Broadcast	Number of broadcast frames with DTIM values.
Tx Success With Retry	Number of frames that were successfully transmitted after being retried.
Tx Multiple retries	Number of frames that were successfully transmitted after being retried multiple times.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Mgmt Frames (PPS)	Rate of retransmitted frames, in packets per second.
Tx Beacons Transmitted	Number of beacons transmitted.
Tx Beacons Transmitted (PPS)	Rate of transmitted beacons, in packets per second.
Tx Probe Responses	Number of transmitted probe responses.
Tx Probe Responses (PPS)	Rate of transmitted probe responses, in packets per second.
Tx Data Transmitted Retried	Number of retried data frames.

Parameter	Description
Tx Data Transmitted	Number of transmitted data frames.
Tx Data Frames	Number of transmitted data frames.
Tx Broadcast Data Frames In	Number of broadcast data frames received by the AP from wired interface to be transmitted in the air.
Tx Data Bytes Transmitted	Total data bytes received by an AP from its wired interface to be transmitted over the air.
Tx Data Bytes	Total data bytes transmitted by the AP over the air.
Tx Time Data Transmitted	Total time on spent successfully transmitting frames (including the retried frames).
Tx Time BC/MC Data	Total time spent transmitting broadcast/multicast frames.
Tx Time Data dropped	Total time spent transmitting dropped frames.
Tx Time Data	Total time spent sending frames received for transmission, including the frames that were dropped after retrying.
Tx Broadcast Data Frames Sent	Broadcast data frames transmitted by the AP.
Tx Broadcast Data Frames Sent (PPS)	Rate of broadcast data frames transmitted by the AP, in packets per second.
Tx Multicast Data Frames	Multicast data frames transmitted by the AP.
Tx Multicast Data Frames (PPS)	Rate of multicast data frames transmitted by the AP, in packets per second.
Tx DMO Multicast	The number of multicast frames transmitted as multicast without converting to unicast.
Tx DMO Invalid	The number of multicast frames which should have been converted but were not as due to invalid format. (This value is typically normally 0.)
Tx DMO Converted	The number of multicast frames received as multicast which were then converted to unicast one or more times. This counter increments once per multicast frame.

Parameter	Description
Tx DMO Replicated	The number of frames transmitted as unicast frames. For each multicast frame the counter is incremented by the number of replications for that frame. (The number of replications is the number of clients associated to the BSSID, VLAN or group receiving these frames).
Tx DMO Dropped	The number of frames dropped as conversion was not consistent with state on the AP. (This value is typically normally 0.)
Tx DMO No Client	Number of times no client was found for an association-ID indicated by the frame. (This value is typically normally 0.)
Tx DMO No BSSID	Number of times the BSSID indicated by the frame was not found. (This value is typically normally 0.)
Tx Unicast Data Frames	Number of transmitted unicast data frames
Tx RTS Success	Number of Ready To Send (RTS) frames successfully transmitted.
Tx RTS Failed	Number of Ready To Send (RTS) frames that were not successfully transmitted
Tx CTS Frames	Number of Clear-to-Send (CTS) frames transmitted.
Tx CTS Frames (PPS)	Rate of CTS frames sent, in packets per second. (This parameter does not include CTS frames send in response to RTS).
Tx Powersave Queue Timeouts	Number of transmit frames discarded from the power save queue because the frames aged out
Tx Dropped After Retry	Number of frames dropped after an attempted retry.
Tx Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Tx Missed ACKs	Number of retries triggered because an acknowledgment was not received.
Tx Failed Beacons	Number of times a radio failed to transmit a beacon at the scheduled interval (100ms).
Tx Multi-Beacon Fail	Number of times multiple consecutive beacons failed to transmit.
Tx Long Preamble	Number of frames sent with a long preamble.
Tx Short Preamble	Number of frames sent with a short preamble.

Parameter	Description
Tx Beacon Interrupts	Number of broadcast beacons that were interrupted.
TX Interrupts	Number of transmission interrupts.
Tx FIFO Underrun	The number of transmitted FIFO overruns.
Tx Allocated Desc	Number of allocated transmit descriptors.
Tx Freed Desc	Number of freed transmit descriptors.
Tx EAPOL Frames	Number of EAPOL frames transmitted
TX STBC Frames	Number of transmitted frames with Space-time block coding (STBC) enabled.
TX LDPC Frames	Number of transmitted frames with Low Density Parity Check (LDPC) enabled.
Tx AGGR Good	Number of aggregated frames successfully transmitted.
Tx AGGR Unaggr	Number of non-aggregate frames transmitted due to unavailability of additional frames for aggregation at the time of transmission.
Tx data <number> Mbps	Number of frames transmitted at the specified rate (in Mbps).
Tx <number> Mbps [Long]	Number of frames with a long preamble transmitted at the specified rate.
Tx <number> Mbps [Short]	Number of frames with a short preamble transmitted at the specified rate.
Tx HT <number> Mbps	Number of high-throughput frames transmitted at the specified rate.
Tx WMM [category]	<p>Number of Wi-Fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command.</p> <ul style="list-style-type: none"> ▪ Tx WMM [BE]: Best Effort ▪ Tx WMM [BK]: Background ▪ Tx WMM [VO]: VoIP ▪ Tx WMM [VI]: Video

Parameter	Description
Tx WMM [category] dropped	Number of dropped Wi-Fi Multimedia (WMM) packets in the following access categories . If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. <ul style="list-style-type: none"> ▪ Tx WMM [BE]: Best Effort ▪ Tx WMM [BK]: Background ▪ Tx WMM [VO]: VoIP ▪ Tx WMM [VI]: Video
Tx UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
TX Timeouts	Number of transmission timeouts
Lost Carrier Events	Number of carrier sense timeouts.
Tx HT40 Hang Detected	Parameter deprecated.
Tx HT40 Hang Stuck	Parameter deprecated.
Tx HT40 Hang Possible	Parameter deprecated.
Tx HT40 Dfs IMM WAR	Number of times the HT 40 RX Clear Hang immunity workaround was employed.
Tx HT40 Dfs HT20 WAR	Number of times the HT 20 RX Clear Hang immunity workaround was employed.
Tx MAC/BB Hang Stuck	Number of times a workaround was employed for potential beacons stuck due to MAC or base-band stuck conditions.
Tx Mgmt Bytes	Total management frame bytes transmitted.
Tx Beacons Bytes	Total number of Beacon frame bytes transmitted.
Tx Data Frames/Bytes 24 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (12-24)
Tx Data Frames/Bytes 36 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (24-36)
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)

Parameter	Description
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI (HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI (FULL)	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz

Parameter	Description
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Tx Data Frames Dropped	Number of transmitted data frames that were dropped.
Tx AMSDU pkt count	Total number of AMSDU bytes transmitted.
Rx Last SNR	The last recorded signal-to-noise ratio.
Rx Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.

Parameter	Description
Rx Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Frames Received	Number of frames received.
Rx Good Frames	Number of frames received with no errors.
Rx Bad Frames	Number of bad or error frames received.
Rx Total Data Frames Recvd	Total number of data frames received.
Rx Total Mgmt Frames Recvd	Total number of management frames received.
Rx Total Control Frames Recvd	Total number of control frames received.
Rx Total Bytes Recvd	Total number of bytes received.
Rx Total Data Bytes Recvd	Total number of data bytes received.
Rx Total RTS Frames Recvd	Total number of Ready-To-Send (RTS) frames received.
Zx Total CTS Frames Recvd	Number of Clear-to-Send (CTS) frames received.
Rx Total ACK Frames	Number of acknowledgment frames received.
Rx Total Beacons Received	Number of beacons received.
Rx Total Probe Requests	Number of probe requests received.
Rx Total Probe Responses	Number of probe responses received.
Rx retry frames	Number of retried frames received.
Channel busy 1s	The percentage of time the radio channel was busy in the last 1 second.
Channel busy 4s	The percentage of time the radio channel was busy in the last 4 seconds.
Channel busy 64s	The percentage of time the radio channel was busy in the last 64 seconds.
Ch Busy perct @ beacon intvl	Percentage of time the channel was busy over the last 30 beacon intervals.

Parameter	Description
Rx Time perct @ beacon intvl	Percentage of time the AP was receiving data over the last 30 beacon intervals.
Rx Discarded Events	Number of non-802.11 events that were detected and discarded during normal operation.
Rx ARM Scan Frames	Number of scan frames sent for the adaptive radio management (ARM) feature.
Rx Data Frames	Number of data frames received.
Rx Data Frames (PPS)	Rate at which data frames were received, in packets per second.
Rx Data Bytes	Number of data bytes received.
Rx Time Data	Total time spent on frames successfully received.
Rx Duplicate Frames	Number of duplicate frames received.
Rx Broadcast Data Frames	Number of broadcast frames received.
Rx Multicast Data Frames	Number of multicast frames received.
Rx Unicast Data Frames	Number of unicast frames received.
Rx Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
Rx Mgmt Frames (PPS)	Rate at which management frames were received, in packets per second.
Rx Control Frames	Number of control frames received.
Rx Control Frames (PPS)	Rate at which control frames were received, in packets per second.
Rx Frames To Me	Number of frames received that are addressed to the specified BSSID.
Rx Bytes To Me	Number of bytes received that are addressed to the specified BSSID.
Rx Time To Me	Total time spent receiving frames sent to a specified BSSID.
Rx Broadcast Frames	Number of broadcast frames received.
Rx Probe Requests	Number of Probe requests received.

Parameter	Description
Rx Probe Requests (PPS)	Rate at which probe requests were received, in packets per second.
Rx RTS Frames	Ready To Send (RTS) frames received. These frames are sent when a computer has data to transmit.
Rx RTS Frames (PPS)	Rate at which RTS frames were received, in packets per second.
Rx CTS Frames	Clear To Send (CTS) frames received. This type of frame are used to verify that a client is ready to receive information.
Rx CTS Frames (PPS)	Rate at which CTS frames were received, in packets per second.
RX PS Poll Frames	Power-Save Poll (PS-Poll) frames received. When a client exits a power-saving mode, it transmits a PS-Poll frame to the AP to retrieve any frames buffered while it was in power-saving mode.
RX CRC Errors	Cyclic Redundancy Check (CRC) is a data sequence that is sent with a frame to help verify if all the data received correctly. Possible CRC error causes include: <ul style="list-style-type: none"> ▪ Hardware malfunction ▪ Loose or unconnected cables ▪ RF interference, such as overlapping access point coverage on a channel or interfering 2.4-GHz signals from devices like microwave ovens ▪ and wireless handset phones
RX PLCP Errors	Physical Layer Convergence Protocol (PLCP) errors.
Rx Frames Dropped	Number of received frames that were dropped.
Rx PHY Events	The number of Physical Layer Events, that are not 802.11 packets, detected by radio as part of its normal receive operation.
Rx RADAR Events	Number of times an AP detects a radar signature. Aruba APs are DFS-compliant detects a radar signature, it will change its channel.
RX Interrupts	The number of receive interrupts received by the CPU from the radio.
RX Overrun	The number of Receive FIFO overruns.
Rx undecryptable	Number of non-decryptable frames received.

Parameter	Description
RX STBC Frames	Number of received frames with STBC enabled.
RX LDPC Frames	Number of received frames with LDPC enabled.
Rx data <number> Mbps	Data packets received at the specified rate (in Mbps).
Rx <number> Mbps	Packets received at the specified rate (in Mbps).
Rx data <number> Mbps	Packets received at the specified rate (in Mbps).
Rx HT <number> Mbps	Number of high-throughput packets received at the specified rate.
Rx WMM [BE]	<p>Number of Wifi Multimedia (WMM) packets received for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command.</p> <ul style="list-style-type: none"> ▪ Rx WMM [BE]: Best Effort ▪ Rx WMM [BK]: Background ▪ Rx WMM [VO]: VoIP ▪ Rx WMM [VI]: Video
RX bad length	Number of frames received with incorrect length.
Rx Null Src MAC	Number of received frames with source MAC address as NULL.
Rx Managment Frames Dropped	Number of received management frames that were dropped.
Rx Data Frames Dropped	Number of received data frames that were dropped.
SNR from CTL0	Signal-to-noise ratio (SNR) on chain 0.
Throttle drops	Number of received frames dropped by AP due to throttling when AP is under high load.
Stop all but Mgmt	Number of data frames dropped because radar was detected on a channel. An AP is allowed to send management frames only and must drop all other frames when radar is detected on a channel.

Command History

Release	Modification
ArubaOS 8.6.0.0	Radio 2 radio ID was introduced for AP-555 access points.
ArubaOS 8.3.0.0	The output of this command was modified to include MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug received-config

```
show ap debug received-config
  ap-name <ap-name> [essid <essid>]
  bssid <bssid> [essid <essid>]
  ip-addr <ip-addr> [essid <essid>]
  ip6-addr <ip6-addr> [essid <essid>]
```

Description

This command shows the configuration the AP downloaded from the managed device.

Parameter	Description
ap-name <ap-name>	Shows log information for an AP with a specific name.
bssid <bssid>	Shows log information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Shows log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows log information for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

The output of this command displays configuration information for each interface. The example below shows only part of the output for this command. Additional parameters not shown in this example are described in the table below.

```
(host) #show ap debug received-config ap-name AP12

Downloaded Config for WIFI 0
-----
Item                               Value
----                               -
BSSID                               00:1a:1e:11:5f:10
LMS IP                              10.6.2.250
Master/Conductor IP                 10.100.103.2
Mode                                AP Mode
QBSS Probe Response                 Allow Access
Native VLAN ID                       1
SAP MTU                             1500 bytes
Heartbeat DSCP                       0
High throughput enable (radio)       Enabled
Channel                             40-
Beacon Period                        100 msec
```

```

Transmit Power                15 dBm
Advertise TPC Capability      Disabled
Enable CSA                    Disabled
CSA Count                     4
Management Frame Throttle interval 1 sec
Management Frame Throttle Limit 20
Active Scan                   Disabled
VoIP Aware Scan               Enabled
Power Save Aware Scan         Enabled
Load aware Scan Threshold     1250000 Bps
40 MHz intolerance           Disabled
Honor 40 MHz intolerance     Enabled
Legacy station workaround     Disabled
Country Code                  US
ESSID                         guest
WMM DSCP Mapping Control     Enabled
...

```

The output of this command includes the following information:

Parameter	Description
BSSID	The BSSID of the AP.
LMS IP	The LMS IP is the IP address of the managed device used by the AP for client data processing.
Master/Conductor IP	IP address of Mobility Conductor, the central configuration and management point for all managed devices.
Mode	Shows the operating modes for the AP. <ul style="list-style-type: none"> ap-mode: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. am-mode: Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
QBSS Probe Response	Quality-of-service BSS (QBSS).
Native VLAN ID	The ID number of the Native VLAN.
SAP MTU	The Maximum Transmission Unit (MTU) for the GRE tunnel.
Heartbeat DSCP	DSCP value for the heartbeat traffic between the AP and the managed device.

Parameter	Description
High throughput enable (radio)	Shows if high-throughput (802.11n) features on tare enabled or disabled on the radio.
Channel	Shows the channel number for the AP's 802.11a/802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Transmit Power	Shows the current transmission power level.
Advertise TPC Capability	If enabled, the AP will advertise its Transmit Power Control (TPC) capability.
Enable CSA	Displays whether or not the AP has enabled channel switch announcements (CSAs) for 802.11h.
CSA Count	Number of channel switch announcements that must be sent before the AP will switch to a new channel.
Management Frame Throttle interval	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero (0), rate limiting is disabled for this AP.
Management Frame Throttle Limit	Maximum number of management frames that can come from this radio in each throttle interval.
Active Scan	Displays whether or not the active scan feature is enabled. This option elicits more information from nearby APs, but also creates additional management traffic on the network. Active Scan is disabled by default, and should <i>not be enabled</i> except under the direct supervision of Aruba Support.
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, VoIP Aware Scan should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that Scanning is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode.

Parameter	Description
Load aware Scan Threshold	The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
Country Code	Display the country code for the AP. The country code specifies allowed channels for that country.
ESSID	An Extended Service Set Identifier (ESSID), for the AP.
Encryption	Encryption type used on this AP.
WPA2 Pre-Auth	802.11x settings are enabled or disabled .
DTIM Interval	Number of beacons that should elapse before an AP sends beacon broadcasts for power save clients.
802.11a Basic Rates	Minimum data rate required for a client to associate with the AP. For an 802.11a radio, this value can be 6, 12 and 24 802.11 data rates. 802.11b/g radios will report a value of 1 and 2 802.11 data rates.
802.11a Transmit Rates	802.11 data rate at which the AP will transmit data to its clients. This value can be 6-54 for 802.11a radios, and 1-54 for 802.11b/g radios.
Station Ageout Time	Number of seconds a station may be idle before it is deauthorized from an AP.
Max Transmit Attempts	maximum number of times the AP will attempt to retransmit data.
RTS Threshold	The minimum packet size at which the AP will issue a request-to-send (RTS) before sending the packet.

Parameter	Description
Max Associations	The maximum number of clients allowed to associated with the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network.
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity time-out threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is enabled or disabled .
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the managed device sends the 802.11 probe responses
Disable Probe Retry	Shows if the AP has enabled or disabled MAC-level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled.
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.

Parameter	Description
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MAC protocol data unit (MPDU) aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on the AP's high-throughput SSID.
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPU within an aggregate MPDU, in microseconds.
Supported MCS set	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.
VLAN	VLAN ID used by the SSID.
Forward mode	Shows the current forward mode (bridge, split-tunnel, or tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). Only 802.1X authentication is supported when configuring bridge or split tunnel mode.
Band Steering	Shows if band-steering has been enabled or disabled for a virtual AP.

Parameter	Description
	<p>ARM's band steering feature encourages dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones.</p> <p>Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40 MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.</p>

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The output will display details of Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug received-log-config

```
show ap debug received-log-config {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows log of configuration received by an AP.

Parameter	Description
ap-name <ap-name>	Shows log of configuration received by specified AP name.
ip-addr <ip-addr>	Shows log of configuration received by an AP for specified IP address.
ip6-addr <ip6-addr>	Shows log of configuration received by an AP for specified IPv6 address.

Example

The following example shows log of configuration received by an AP named ap-205:

```
(host) [mynode] #show ap debug received-log-config ap-name ap-205

AP log level config
-----
Facility  Level      Sub Category  Level
-----  -
arm       warnings
network   warnings
security  warnings   ids           warnings
security  warnings   ids-ap        warnings
system    warnings
user      warnings
wireless  warnings
Log level config version :1

AP debug level config
-----
Facility  Level  Debug value  Sub Category
-----  -
Debug log config version :1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug received-reg-table

```
show ap debug received-reg-table {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows downloaded regulatory table for an AP.

Parameter	Description
ap-name <ap-name>	Shows downloaded regulatory table for a specified AP name.
bssid <bssid>	Shows downloaded regulatory table for a specified BSSID.
ip-addr <ip-addr>	Shows downloaded regulatory table for a specified IP address.
ip6-addr <ip6-addr>	Shows downloaded regulatory table for a specified IPv6 address.

Example

The following example shows downloaded regulatory table for an AP named ap-205 (For versions prior to ArubaOS 8.9.0.0).

```
(host) [mynode] #show ap debug received-reg-table ap-name ap-205

Country reg-info for Country Code "US"
-----
PHY Type                Allowed Channels
-----
802.11g (indoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 132 136
140 144 149 153 157 161 165
802.11g (outdoor)       1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)       52 56 60 64 100 104 108 112 116 132 136 140 144 149
153 157 161 165
802.11g 40MHz (indoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)  36-40 44-48 52-56 60-64 100-104 108-112 132-136
140-144 149-153 157-161
802.11g 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor) 52-56 60-64 100-104 108-112 132-136 140-144 149-153
157-161
802.11a 80MHz (indoor)  36-48 52-64 100-112 132-144 149-161
802.11a 80MHz (outdoor) 52-64 100-112 132-144 149-161
802.11a (DFS)           52 56 60 64 100 104 108 112 116 132 136 140 144

Certificate reg-info for AP-205 Country Code "US"
-----
```

```

PHY Type                Allowed Channels
-----
802.11g (indoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 132 136
140 144 149 153 157 161 165
802.11g (outdoor)       1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)       52 56 60 64 100 104 108 112 116 132 136 140 144 149
153 157 161 165
802.11g 40MHz (indoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)  36-40 44-48 52-56 60-64 100-104 108-112 132-136
140-144 149-153 157-161
802.11g 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor) 52-56 60-64 100-104 108-112 132-136 140-144 149-153
157-161
802.11a 80MHz (indoor)  36-48 52-64 100-112 132-144 149-161
802.11a 80MHz (outdoor) 52-64 100-112 132-144 149-161
802.11a (DFS)           52 56 60 64 100 104 108 112 116 132 136 140 144

Max EIRP settings for AP-205 Country Code "US"
-----
Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 36 40 44
48 52 56 60 64 100 104 108 112 116 120 124 128 132 136
140 144 149 153 157 161 165
-----
- - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - -
b          29 29 29 29 29 29 29 29 29 29 29 * * * * *
* * * * *
* * * * *
g/a        32 32 32 32 32 32 32 32 32 32 32 * * * 21 21 21
21 28 28 28 28 28 28 28 28 28 28 * * * 27 27 27
27 33 33 33 33 33
HT 20      32 32 32 32 32 32 32 32 32 32 32 * * * 21 21 21
21 27 28 28 28 28 28 28 28 28 28 * * * 27 27 27
27 33 33 33 33 33
HT 40      32 32 32 32 32 32 32 32 32 32 32 * * * 20 20 20
20 24 24 24 24 24 24 24 24 24 * * * 24 24 24
23 32 32 32 32 32
VHT 80     * * * * * * * * * * * * * * * 21 21 21
21 21 21 21 21 21 21 21 21 21 * * * * 21 21 21
20 33 33 33 33 33
country    36 36 36 36 36 36 36 36 36 36 36 * * * 23 23 23
23 30 30 30 30 36 36 36 36 36 * * * 36 36 36
36 36 36 36 36
DFS        * * * * * * * * * * * * * * * * * *
* FCC FCC FCC FCC FCC FCC FCC FCC FCC * * * FCC FCC
FCC FCC * * * * *

```

The following example shows a portion of the downloaded regulatory table for an AP named hhm-635 (ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap debug received-reg-table ap-name hhm-635
Country reg-info for Country Code "US"

```

```

-----
PHY Type                Allowed Channels
-----
802.11g (indoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 120
124 128 132 136 140 144 149 153 157 161 165
802.11g (outdoor)       1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)       36 40 44 48 52 56 60 64 100 104 108 112 116 120
124 128 132 136 140 144 149 153 157 161 165
802.11g 40MHz (indoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)  36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
802.11g 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor) 36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
802.11a 80MHz (indoor)  36-48 52-64 100-112 116-128 132-144 149-161
802.11a 80MHz (outdoor) 36-48 52-64 100-112 116-128 132-144 149-161
802.11a 160MHz (indoor) 36-64 100-128
802.11a 160MHz (outdoor) 36-64 100-128
802.11a (DFS)           52 56 60 64 100 104 108 112 116 120 124 128 132
136 140 144
6g (indoor)             1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69
73 77 81 85 89 93 121 125 129 133 137 141 145 149 153 157 161 165 169 173
177 181 185
6g (outdoor)            1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69
73 77 81 85 89 93 121 125 129 133 137 141 145 149 153 157 161 165 169 173
177 181 185
6g 40MHz (indoor)       1-5 9-13 17-21 25-29 33-37 41-45 49-53 57-61 65-69
73-77 81-85 89-93 121-125 129-133 137-141 145-149 153-157 161-165 169-173
177-181
6g 40MHz (outdoor)      1-5 9-13 17-21 25-29 33-37 41-45 49-53 57-61 65-69
73-77 81-85 89-93 121-125 129-133 137-141 145-149 153-157 161-165 169-173
177-181
6g 80MHz (indoor)       1-13 17-29 33-45 49-61 65-77 81-93 129-141 145-157
161-173
6g 80MHz (outdoor)      1-13 17-29 33-45 49-61 65-77 81-93 129-141 145-157
161-173
6g 160MHz (indoor)      1-29 33-61 65-93 129-157
6g 160MHz (outdoor)    1-29 33-61 65-93 129-157

```

Certificate reg-info for AP-635 Country Code "US"

```

-----
PHY Type                Allowed Channels
-----
802.11g (indoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 120
124 128 132 136 140 144 149 153 157 161 165
802.11g (outdoor)       1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)       36 40 44 48 52 56 60 64 100 104 108 112 116 120
124 128 132 136 140 144 149 153 157 161 165
802.11g 40MHz (indoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)  36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161
802.11g 40MHz (outdoor) 1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor) 36-40 44-48 52-56 60-64 100-104 108-112 116-120
124-128 132-136 140-144 149-153 157-161

```

```

802.11a 80MHz (indoor)    36-48 52-64 100-112 116-128 132-144 149-161
802.11a 80MHz (outdoor) 36-48 52-64 100-112 116-128 132-144 149-161
802.11a 160MHz (indoor)  None
802.11a 160MHz (outdoor) None
802.11a (DFS)           52 56 60 64 100 104 108 112 116 120 124 128 132
136 140 144
6g (Lp_indoor)          1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69
73 77 81 85 89 93 97 101 105 109 113 117 121 125 129 133 137 141 145 149 153
157 161 165 169 173 177 181 185 189 193 197 201 205 209 213 217 221 225 229
6g 40MHz (Lp_indoor)    1-5 9-13 17-21 25-29 33-37 41-45 49-53 57-61 65-69
73-77 81-85 89-93 97-101 105-109 113-117 121-125 129-133 137-141 145-149
153-157 161-165 169-173 177-181 185-189

```

Command History

Release	Modification
ArubaOS 8.9.0.0	The 6g value was introduced under <code>PHY Type</code> output parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug scan-settings

```
show ap debug scan-settings {ap-name <ap-name>}{{ip-addr <ip-addr>}}{ip6-addr <ip6-addr>}
```

Description

This command shows radio scanning of an AP.

Parameter	Description
ap-name <ap-name>	Shows radio scanning of an AP for specified AP name.
ip-addr <ip-addr>	Shows radio scanning of an AP for specified IP address.
ip6-addr <ip6-addr>	Shows radio scanning of an AP for specified IPv6 address.

Example

The following example shows radio scanning of an AP named ap-205:

```
(host) [mynode] #show ap debug scan-settings ap-name ap-205
```

```
Radios Scan-setting
```

```
-----  
Radio Index  Status  
-----
```

```
0             Enable  
1             Enable
```

The following example shows radio scanning of an AP-555 ,

```
(host) #show ap debug scan-settings ap-name AP555-0
```

```
Radios Scan-setting
```

```
-----  
Radio Index  Status  
-----
```

```
0             Enable  
1             Enable  
2             Enable
```

Command History

Release	Modification
ArubaOS 8.6.0.0	The output will display the status of Radio 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug ses-esl-log

```
show ap debug ses-esl-log {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the SES-Imagatog's ESL server logs for an AP.

Parameter	Description
ap-name <ap-name>	The name of the AP.
ip-addr <ip-addr>	The IP address of the AP.
ip6-addr <ip6-addr>	The IPv6 address of the AP.

Examples

The following example shows the SES-Imagatog's ESL server logs for an AP:

```
(Host) *[mynode] (config) #show ap debug ses-esl-log ap-name AP32x_03
[11572]2018-12-14 05:32:50 Startup summary(local config):
[11572]2018-12-14 05:32:50 Ap-Id configured via CLI: false
[11572]2018-12-14 05:32:50 Target serial device: /dev/ttyUSB0
[11572]2018-12-14 05:32:50 Sync Protocol version: 0
[11572]2018-12-14 05:32:50 Max. window size: 14
[11572]2018-12-14 05:32:50 Output power: C
[11572]2018-12-14 05:32:50 Max. output power: A
[11572]2018-12-14 05:32:50 Always force firmware update: true
[11572]2018-12-14 05:32:50 TCP listen port: 7353
[11572]2018-12-14 05:32:50 SSL enabled: false
[11572]2018-12-14 05:32:50 Control channel disabled: false
[11572]2018-12-14 05:32:50 Connection-mode: Outbound
[11572]2018-12-14 05:32:50 Apc-address:
[11572]2018-12-14 05:32:50 Apc-port: 7353
[11572]2018-12-14 05:32:50 Coex. level: full
[11572]2018-12-14 05:32:50 Coex. signal shift (micros): -6000
[11572]2018-12-14 05:32:50 Coex. signal covers for jitter enabled: true
[11572]2018-12-14 05:32:50 Coex. signal additional covering (micros): 2000
[11572]2018-12-14 05:32:50 Startup summary(protocol config):
[11572]2018-12-14 05:32:50 Batch-Size: 16
[11572]2018-12-14 05:32:50 Threshold: 32
[11572]2018-12-14 05:32:50 Communication restart sync batches slot jump
multiplier: 3
[11572]2018-12-14 05:32:50 Number of buffered sync batches: 2
[11572]2018-12-14 05:32:50 Sync buffer size: 64
[11572]2018-12-14 05:32:50 Sync max. slot offset: 320
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
AP-303H, 300 Series access points, 310 Series access points, 320 Series access points, 330 Series access points, 340 Series access points, and 510 Series access points	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug shaping-table

```
show ap debug shaping-table {ap-name <ap-name>|ip-addr <ip-addr>}
```

Description

This command shows shaping information for clients associated to an AP.

Parameter	Description
ap-name <ap-name>	Show shaping table information for a specific AP.
ip-addr <ip-addr>	Show shaping table information for a specific AP IP address by entering its IP address in dotted-decimal format.

Example

The following command shows the shaping table of an AP named ap22.

```
(host) #show ap debug shaping-table ap-name ap22

VAP station000
pktin  pktout  pktdrop  pktqd   cmn[C:O:H]   drop   Numcl  TotCl
BWmgmt
0        0         0         0       0-0-0   0-0     0-0-0   0       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0        0         0         0       0        0        0        0        0

idx      tokens  last-t  in      out      drop    q       tx-t    rx-t    al-t
rate
idx      d1      d2      d3      d4      d5      d6      d7      d8      d9
0        0         0         0         0         0         0         0         0         0

VAP station001
pktin  pktout  pktdrop  pktqd   cmn[C:O:H]   drop   Numcl  TotCl
BWmgmt
0        8144    0         0       0-0-0   0-0     0-2-0   2       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0        0         0         0         0         0         0         0         0

idx      tokens  last-t  in      out      drop    q       tx-t    rx-t    al-t
rate
1        0         0         0       2966    0        0       716     0        0
0
3        0         0         0         31      0        0        8       0        0
0
```

idx	d1	d2	d3	d4	d5	d6	d7	d8	d9
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0

The output of this command includes the following information:

Column	Description
pktin	Number of packets received by the AP.
pktout	Number of packets sent by the AP.
pktdrop	Number of packets dropped by the AP.
pktqd	Number of packets queued.
drop	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
Numcl	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
TotCl	Total number of clients associated with the AP
Bwmgmt	This data column displays a 1 if the bandwidth management feature has been enabled. Otherwise, it displays a 0.
idx	Association ID.
tokens	This value represents the credits the station has to transmit tokens.
last-t	Number of tokens that were allocated to the station last time token allocation algorithm ran.
in	Number of packets received.
out	Number of packets sent.
drop	Number of dropped packets.
q	Number of queued packets
tx-t	Total time spent transmitting data.
rx-t	Total time spent receiving data.
al-t	Total time allocated for transmitting data to this station.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug spanning-tree

Syntax

```
show ap debug spanning-tree {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

This command shows an AP's spanning tree statistics.

Parameter	Description
ap-name <ap-name>	Show log information for an AP with a specific name.
bssid <bssid>	Show log information for a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show log information for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

The following command shows the AP debug spanning tree state.

```
(host) [mynode] #show ap debug spanning-tree
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug sta-msg-stats

Syntax

```
show ap debug sta-msg-stats {[ap-name <ap-name>] [bssid <bssid>]}
```

Description

This command shows AP-STM to STM message statistics.

Parameter	Description
ap-name <ap-name>	Shows AP-STM to STM message statistics for specified AP name.
bssid <bssid>	Shows AP-STM to STM message statistics for specified BSSID.

Example

The following example shows AP-STM to STM message statistics for BSSID d8:c7:c8:38:fc:f5:

```
(host) [mynode] #show ap debug sta-msg-stats bssid d8:c7:c8:38:fc:f5

STA Up/Down Message Counters for BSSID d8:c7:c8:38:fc:f5
-----
Name                                     Value
----                                     -
STA Messages: Up Down                   0 0
Dup Seqnum                               0
Success: Assoc Re-Assoc                 0 0
STA Not found Errors                     UP: 0 DN 0
Assoc Rejections: Total BLIST CAC VLAN AID ALLOC FT 0 0 0 0 0 0 0
Dormant Clear Skipped                   0

STA Up/Down Message Counters
-----
Num Messages Received
0
-----
-
Messages Received per slot
0 0 0
STA Messages: Up Down Total
0 0 0
Success: Assoc Re-Assoc AcksSent
0 0 0
Unpack Errors
0
```

```
Not found Errors: sta sap; sta_alloc
UP: 0 0 DN: 0 0; alloc_err=0
Duplicate Sequence Num, Auth Busy Drops
0, 0
Assoc Rejections: Total UAC BLIST CAC VLAN AID ALLOC FT TIME CTRMSR SCTRMSR
0 0 0 0 0 0 0 0 0 0 0 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug stm-trace

show ap debug stm-trace

Description

This command shows the debug trace settings for STM.

Example

The following example shows the debug trace settings for STM:

```
(host) [mynode] #show ap debug stm-trace

STM Debug tracing: Categories=All; loglevel=INFO; mac_filter=not set; ip_
filter=not set
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug switching

Syntax

```
show ap debug switching {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows an AP's switching statistics.

Parameter	Description
ap-name <ap-name>	Name of the access point.
ip-addr <ip-addr>	IP address of the access point.
ip6-addr <ip6-addr>	IPv6 address of the access point.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug system-status

```
show ap debug system-status
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows detailed system status information for an AP.

Parameter	Description
ap-name <ap-name>	Show system status data for an AP with a specific name.
bssid <bssid>	Show system status data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
ip-addr <ip-addr>	Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Issue this command under the guidance of Aruba technical support to troubleshoot network issues. The output of this command displays the following types of information (if it exists) for the selected AP:

■ Bootstrap information	■ Per-radio statistics	■ Ethernet duplex/speed settings
■ Descriptor Usage	■ Encryption statistics	■ Tunnel heartbeat stats
■ Interface counters	■ AP uptime	■ Boot version
■ MTU discovery	■ Memory usage	■ LMS information
■ ARP cache	■ Kernel slab statistics	■ Power status
■ Route table	■ Interrupts	■ CPU type
■ Interface Information	■ Crash Information	■ CPU usage statistics
■ System Status Script	■ Radio profile name	■ Dual 5 GHz mode
■ NSS CPU Usage		

Power Status

The following lines under power status indicate the power status of the AP:

- **Operational State** indicates the current state of the AP, that is, as seen with the power light on the AP. **Operational State** may be different from **Current HW State** as a result of LLDP negotiation.
- **Current HW State** indicates the result from POE negotiation in hardware.
- **LLDP Negotiated POE Power** indicates the LLDP negotiated power.

The following parameters are included in the output of this command, and can help troubleshoot problems on an AP or wireless network.

Parameter	Description
The Failed column in the Descriptor Usage section	This parameter can tell you if the AP is dropping packets.
Interface Information table	This parameter can tell you if the Ethernet network is working properly. This table should not show an excessive number of errors.
AP Uptime table	Low values in this table can indicate problems with the wired network, or with the AP itself.
Tunnel Heartbeat table	This table can indicate the health of the underlying wired network.
Rebootstrap Information table / Reboot Information table	A large number of reboots can mean that the AP has hardware problems.

Example

The following example shows the NSS CPU usage of an AP:

```
(host) [mynode] #show ap debug system-status ap-name XXX
NSS CPU usage
-----
CPU Utilization:
Note: Averaged over 1 second
Core 0:
Min      Avg      Max
3%       5%       8%
```

Command History

Release	Modification
ArubaOS 8.8.0.0	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ■ A new output parameter, <code>NSS CPU Usage</code> was introduced. The NSS CPU usage will be displayed only for AP-534, AP-535, and AP-555 access points. ■ The output of the command was modified to display Ethernet related details.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug trace-addr

show ap debug trace-addr

Description

This command shows MAC addresses in the trace buffer. Use this command to troubleshoot wireless clients that are being traced for 802.11 communication.

Examples

The output of the command shows the **Trace List** table. If no wireless clients are being traced, this table will be empty.

```
(host) #show ap debug trace-addr

Trace List
-----
MAC Address
-----
00:1a:1e:c5:ca:b4
00:1a:1e:c5:d6:46
00:1a:1e:c5:d7:40
00:1a:1e:c5:d7:64
00:1a:1e:c5:d9:56
00:1a:1e:c5:d9:b0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug tunnel-id

show ap debug tunnel-id

Description

This command shows all tunnel IDs stored in STM.

Example

The following example shows all tunnel IDs stored in STM:

```
(host) [mynode] #show ap debug tunnel-id

List of Tunnel id
-----
Hash Table  Tunnel id  IP Address
-----
SAP Hash    65548      10.15.147.180
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap debug usb

```
show ap debug usb
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the USB information provisioned on the RAP.

Parameter	Description
ap-name <ap-name>	Show system status data for an AP with a specific name.
ip-addr <ip-addr>	Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Examples

The output of the command shows the USB information provisioned on the RAP.

```
(host) #show ap debug usb ap-name RAP2
USB Information
-----
Parameter                               Value
-----
Manufacturer                             Pantech,
Product                                  PANTECH
Serial Number
Driver                                   ptuml_cdc_ether
Vendor ID                                 106c
Product ID                                3718
USB Modem State                           Active
USB Uplink RSSI(in dBm)                   -73
Supported Network Services                 CDMA GSM LTE
Firmware Version                           L0290VWB522F.242
ESN Number                                 990000472325325
Current Network Service                    4G-LTE
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap debug usb-device-mgmt

```
show ap usb-device-mgmt
  ap-name <ap-name> {device all|module all|plugin {all|detail <plugin-name>}|rule
  all|subscriber {all|detail <service-type>}}
  ip-addr <ip-addr> {device all|module all|plugin {all|detail <plugin-name>}|rule
  all|subscriber {all|detail <service-type>}}
  ip6-addr <ip6-addr> {device all|module all|plugin {all|detail <plugin-name>}|rule
  all|subscriber {all|detail <service-type>}}
  log
```

Description

This command shows debugging information of USB devices managed on an AP.

Parameter	Description
ap-name <ap-name>	Show debugging information of USB devices managed on an AP that is specified by the AP name.
ip-addr <ip-addr>	Show debugging information of USB devices managed on an AP that is specified by the IP address.
ip6-addr <ip6-addr>	Show debugging information of USB devices managed on an AP that is specified by the IPv6 address.
log	Show debugging log of USB devices managed by an AP that is specified by AP name, IP address, or IPv6 address.
device all	Show device debugging information of all USB devices managed by an AP.
module all	Show module debugging information of USB devices managed by an AP.
plugin {all detail <plugin-name>}	Show plugin debugging information of USB devices managed by an AP.
rule all	Show rule debugging information of USB devices managed by an AP.
subscriber {all detail <service-type>}	Show subscriber debugging information of USB devices managed by an AP.

Example

The following command shows the debug statistics of USB devices managed on an AP that is specified by AP name:

```
(host) [mynode] #show ap debug usb-device-mgmt ap-name 325 device all

USB Device Table
-----
Device ID  Manufacturer  Product  Serial Number  Version  VendorID
ProductID  Revision  Class  Device  Flags  Relationship  Driver  Up Time
-----
- - - - -
No USB device.
```

Related Commands

Command	Description
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap usb-prof	Shows configuration for AP USB profile.
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
ap usb-acl-prof	Configures AP USB ACL profile.
ap usb-profile	Configures AP USB profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable Mode.

show ap debug usb-modem-log

```
show ap debug usb-modem-log
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command displays the USB modem logs of an AP. Use this command to view the USB information provisioned on the RAP.

Parameter	Description
ap-name <ap-name>	Shows system status data for an AP with a specific name.
ip-addr <ip-addr>	Shows system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Examples

The output of the command shows the USB information provisioned on the RAP.

```
(host) #show ap debug usb ap-name RAP2
USB Information
-----
Parameter                               Value
-----
Manufacturer                             Pantech,
Product                                  PANTECH
Serial Number
Driver                                    ptuml_cdc_ether
Vendor ID                                 106c
Product ID                                3718
USB Modem State                            Active
USB Uplink RSSI(in dBm)                    -73
Supported Network Services                 CDMA GSM LTE
Firmware Version                           L0290VWB522F.242
ESN Number                                 990000472325325
Current Network Service                     4G-LTE
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap dot1x

```
debug log
information
status
```

Description

This command displays the details about an 802.1X AP.

Parameter	Description
debug log	Displays the debug logs of an 802.1X AP.
information	Displays the PEAP, TLS, and authentication related information of an 802.1X AP.
status	Displays the status of an 802.1X AP.

Command History

Release	Modification
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap dot1x debug log

```
show ap dot1x debug log {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

This command displays the debug logs of an 802.1X AP.

Parameter	Description
ap-name <ap-name>	Shows data for an AP with a specific name.
bssid <bssid>	Shows data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address.
ip-addr <ip-addr>	Shows data for an AP with a specific IP address.

Example

The following example displays the debug logs of an 802.1X AP.

```
(host) [mynode] #show ap dot1x information ap-name ap325show ap dot1x debug
log ap-name ap325
Output wpa_supPLICANT debug-log content here.
```

Command History

Command	Description
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap dot1x information

```
show ap dot1x information {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

This command displays the PEAP, TLS, and authentication related information of an 802.1X AP.

Parameter	Description
ap-name <ap-name>	Shows data for an AP with a specific name.
bssid <bssid>	Shows data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address.
ip-addr <ip-addr>	Shows data for an AP with a specific IP address.

Example

The following example displays the PEAP, TLS, and authentication related information about an 802.1X AP.

```
(host) [mynode] #show ap dot1x information ap-name ap325
AP 802.1X PEAP Username: Aruba
AP 802.1X TLS: Disabled
AP 802.1X TLS Suffix: Disabled
AP 802.1X TLS Suffix Domain: aruba.ap
AP 802.1X Authentication timeout bypass: Enabled
AP 802.1X Authentication timeout retires: 3
```

Command History

Command	Description
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap dot1x status

```
show ap dot1x status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

This command displays the status of an 802.1X AP.

Parameter	Description
ap-name <ap-name>	Shows data for an AP with a specific name.
bssid <bssid>	Shows data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address.
ip-addr <ip-addr>	Shows data for an AP with a specific IP address.

Example

The following example displays the status of an 802.1X AP.

```
(host) [mynode] #show ap dot1x status ap-name ap325
AP 802.1X Type: PEAP
AP 802.1X Authentication result: Success
Authentication Statistics:
Authenticator ready number: 1
Authentication success number: 1
Authentication failure number: 0
Authentication timeout number: 0
```

Command History

Command	Description
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap deploy-profile

```
show ap deploy-profile
```

Description

This command shows if the AP deploy profile is enabled or not. It also displays if the policy is applied on default AP group, status of the blacklist/denylist policy and the complete list of IPv4 and IPv6 address ranges to which the AP deployment policy is applied.

Example

The following command displays the status of the AP deploy profile and various configurations applied on the profile:

```
(host) [mynode] #show ap deploy-profile

Profile enabled: no
Apply to default ap group: no
Blacklist/Denylistenabled: yes

AP deploy policy IP range Table
-----
Starting IP   Ending IP
-----
1.1.1.1      1.1.1.10

AP deploy policy IPv6 range Table
-----
Starting IP   Ending IP
-----
::3          ::5
2016::1      2016::10
2016::15     2016::15
```

Related Commands

Command	Description
ap deploy-profile	This command applies the AP deployment policy to the default AP group, and/or to the list of AP MAC addresses included in the UAP blacklist/denylist table, and/or to the specified IP address range. The AP deployment policy redirects the applicable APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap details

```
show ap details [advanced] {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|wired-mac <wired-mac>}
```

Description

This command shows the detailed provisioning parameters, hardware, and operating information for a specific AP.

Parameter	Description
advanced	Shows additional information of specified AP. Include the following additional data in the output of this command: <ul style="list-style-type: none">■ Switch message counts■ AP group information■ Virtual AP operating information
ap-name <ap-name>	Show data for a specific AP by entering the name of the AP for which you want to display information.
ip-addr <ip-addr>	Show data for an AP with the specified IP address.
ip6-addr <ip6-addr>	Show data for an AP with the specified IPv6 address.
wired-mac <wired-mac>	Show mac address of an AP.

Examples

The following example shows part of the output for the command `show ap details advanced ap-name <ap-name>`.

```
(host)[node] #show ap details advanced ap-name ap-205
AP "ap-205" Basic Information
-----
Item                Value
----                -
AP IP Address       191.191.191.252
LMS IP Address      192.192.189.1
Group               default
Location Name       N/A
Status              Up
Up time             19d:13h:30m:19s

AP "ap-205" Hardware Information
-----
Item                Value
----                -
AP Type             205
Serial #            CM0487514
Wired MAC Address   40:e3:d6:cf:61:96
```

```

Radio 0 BSSID      40:e3:d6:76:19:70
Radio 1 BSSID      40:e3:d6:76:19:60
Enet 1 MAC Address N/A
Enet 2 MAC Address N/A
Enet 3 MAC Address N/A
Enet 4 MAC Address N/A
Enet 5 MAC Address N/A
Enet 6 MAC Address N/A
Enet 7 MAC Address N/A

AP "94:b4:0f:c0:d0:86" Radio[0] Eirp(max, min, offset) Information
-----
Item           Value      Source
Eirp max       33        Netinsight
Eirp min       2         Netinsight
Eirp offset    3         Netinsight

AP "94:b4:0f:c0:d0:86" Radio[1] Eirp(max, min, offset) Information
-----
Item           Value      Source
Eirp max       19        Netinsight
Eirp min       9         Netinsight
Eirp offset    -6        Netinsight

```

The following example shows part of the output for the command `show ap details ap-name <ap-name>`.

```

(host) [mynode] #show ap details ap-name ap-205

AP "ap-205" Basic Information
-----
Item           Value
-----
AP IP Address   191.191.191.252
LMS IP Address  192.192.189.1
Group           default
Location Name   N/A
Status          Up
Up time         19d:13h:30m:19s

AP "ap-205" Hardware Information
-----
Item           Value
-----
AP Type        205
Serial #       CM0487514
Wired MAC Address 40:e3:d6:cf:61:96
Radio 0 BSSID   40:e3:d6:76:19:70
Radio 1 BSSID   40:e3:d6:76:19:60
Enet 1 MAC Address N/A
Enet 2 MAC Address N/A
Enet 3 MAC Address N/A
Enet 4 MAC Address N/A
Enet 5 MAC Address N/A
Enet 6 MAC Address N/A
Enet 7 MAC Address N/A

Starting from ArubaOS 8.3.0.0, this command displays the new statistics on
AP recovery mode:
(host) [node] #show ap details ap-name <ap-name>

```

```

AP "<ap-name>" Radio 0 Operating Information
-----
Item                Value      Source
-----
Very High throughput Enabled   Configuration
High throughput     Enabled   Configuration
Mode                AP        Configuration
Band                802.11a
Primary Channel     36       Configuration
80MHz Channel Group 36-48    Configuration
EIRP                10.0     Configuration
Fast recovery start 2017-03-09 11:57:56
Fast recovery end  2017-03-09 11:58:00
Fast recovery    1

```

The output of this command includes the following information:

Parameter	Description
AP IP Address	IP address of the AP
LMS IP Address	The IP address of the local management switch (LMS)—the Aruba controller which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
Group	Name of the AP's AP group.
Location Name	Location of the AP.
Status	Current status of the AP, either Up or Down .
Up time	Number of hours, minutes and seconds since the last controller reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
AP Type	AP model
Serial #	Serial number for the AP
Wired MAC address	MAC address of the wired interface.
Radio 0 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 0. This is usually the radio's MAC address.
Radio 1 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 1. This is usually the radio's MAC address.
Radio 2 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 2. This is usually the radio's MAC address.

Parameter	Description
Enet 1 MAC address	MAC address of the Ethernet1 port of AP.
Enet 3 MAC address	MAC address of the Ethernet3 port of AP.
Enet 4 MAC address	MAC address of the Ethernet4 port of AP.
Enet 5 MAC address	MAC address of the Ethernet5 port of AP.
Enet 6 MAC address	MAC address of the Ethernet6 port of AP.
Enet 7 MAC address	MAC address of the Ethernet7 port of AP.
Fast recovery start	Start date and time of the AP Fast Recovery process.
Fast recovery end	End date and time of the AP Fast Recovery process.
Fast Recovery	Number of Fast Recoveries that happened in the AP.

The following example shows the output of the `show ap details advanced ip-addr <ip-addr>` command, where a controller ages out an AP:

```
(host)[node] #show ap details advanced ip-addr 10.3.90.17
AP "9c:1c:12:c0:86:5a" Basic Information
-----
Item                                     Value
----                                     -
AP IP Address                           10.65.39.245
LMS IP Address                           10.65.38.93
Group                                    test-rap
Location Name                            N/A
Status                                    Up
Up time                                  4d:8h:39m:23s
AP Flags:                                ; Licensed; Ready for
Standby; Standby Not Connected
Installation                              indoor
max delay between msgs, cfgs:            4710, 4710
ap RTT total, hiwmk:                     29, 10
Currently in reglist                      No
Reglist Entries, Exits:                  1702 1702
time in reglist total, hiwmk:            14 1
calls to bulk_reg, reg_single:           1702 5062
inter registration gap total, hiwmk:     376439 4710
VAP registration errs, retries:          0 0
VAP Registration Requests, Responses, Re-Requests: 3360 3360 0
registration batch size                  6
SACC registration Requests, Responses    0 0
SACC registration errs, retries:         0 0
ACL msgsz adaptations                    0
Max Nodes                                 unlimited
LMS macid                                 00:0b:86:9a:04:17

AP "9c:1c:12:c0:86:5a" Licensing Information
```

```

-----
Item                                     Value
-----
AP License Total Increments             179
AP License Total Decrements             178
AP License Total Active Increments      179
AP License Total Active Decrements      178
AP License Total Standby Increments      0
AP License Total Standby Decrements      0
AP Total GSM Standby Update Counter      0
Current AP License Total Increments      1
Current AP License Total Decrements      0
Current AP License Active Increments     1
Current AP License Active Decrements     0
Current AP License Standby Increments    0
Current AP License Standby Decrements    0
Current AP GSM Standby Update Counter    0
Current AP GSM Info                      44/4/0/0

```

Rebootstraps and Control Messages Log

```

-----
Recent Messages                          Time now: Tue Jun 26 04:38:31 2018
-----
Time Offset                              Message details
-----
-195                                     RCVD: STATUS_REPORT len=57 peer=10.65.39.245 seq_
num=2949 rtt=0 result=OK
-200                                     SENT: CONFIG len=351 peer=10.65.39.245 seq_
num=1867 tries=1 rtt=0 result=OK
-200                                     RCVD: CHAN_PWR_CHANGE len=30 peer=10.65.39.245
seq_num=2948 rtt=0 result=OK

```

```

Rebootstrap                              Thu Jun 21 20:01:11 2018
Time Offset                              Message details
-----
-0                                       RCVD: HELLO len=1410 peer=10.65.39.245 seq_num=0
rtt=0 result=OK
-337                                     SENT: ACL_CONFIG len=333 peer=10.65.39.245 seq_
num=108 tries=1 rtt=-1
-347                                     SENT: ACL_CONFIG len=333 peer=10.65.39.245 seq_
num=108 tries=1 rtt=-1

```

```

Rebootstrap                              Thu Jun 21 19:55:03 2018
Time Offset                              Message details
-----
-0                                       RCVD: HELLO len=1435 peer=10.65.39.245 seq_num=0
rtt=0 result=OK
-49                                     SENT: ACL_CONFIG len=335 peer=10.65.39.245 seq_
num=101 tries=1 rtt=-1
-59                                     SENT: ACL_CONFIG len=335 peer=10.65.39.245 seq_
num=101 tries=1 rtt=-1

```

```

Rebootstrap                              Thu Jun 21 19:53:44 2018
Time Offset                              Message details
-----
-0                                       RCVD: HELLO len=1435 peer=10.65.39.245 seq_num=0

```

```

rtt=0 result=OK
-48          SENT: FW_CONFIG len=664 peer=10.65.39.245 seq_
num=15 tries=3 rtt=-1
-70          SENT: CLEAR_FW_CONFIG len=101 peer=10.65.39.245
seq_num=14 tries=1 rtt=0 result=OK

Info of last session
Last heartbeat seq number  28
Reason for disconnect      Deleted by SAPM(KEEPALIVE timeout)
Timestamp                  2018-06-21 19:55:43

```

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.6.0.0	A new output parameter <code>Radio 2 BSSID</code> was introduced.
ArubaOS 8.4.0.0	<ul style="list-style-type: none"> ■ The Reason for disconnect field was added to the output of the <code>show ap details advanced ip-addr <ip-addr></code> command. ■ The output of the <code>show ap details advanced ap-name <ap-name></code> command was modified to display Eirp (max, min, offset) information.
ArubaOS 8.3.0.0	Additional statistics on AP Fast Recovery was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor and Enable mode on Managed Device.

show ap enet-link-profile

```
show ap enet-link-profile [<profile>]
```

Description

This command shows a list of all Ethernet Link profiles. Include a profile name to display details for the specified Ethernet Link Profile, or omit the <profile> parameter to display a list of all Ethernet Link profiles.

Example

This command shows the speed of the Ethernet interface and the current duplex mode for the Ethernet Link profile "default":

```
(host) [mynode] #show ap enet-link-profile default

AP Ethernet Link profile "default"
-----
Parameter  Value
-----  -
Speed                auto
Duplex              auto
802.3az (EEE)       Disabled
802.3bz             Yes
Power over Ethernet Disabled
The output of this command includes the following parameters:
```

Parameter	Description
Speed	The speed of the Ethernet interface. This value can be either 10 Mbps , 100 Mbps , 1000Mbps (1 Gbps), or auto (auto-negotiated).
Duplex	The duplex mode of the AP's Ethernet interface. This value can be either full , half , or auto (auto-negotiated).
802.3az	This displays if the support for the 802.3az Energy Efficient Ethernet (EEE) standard is enabled.
802.3bz	This displays if the support for IEEE 802.3bz standard is enabled.
Power Over Ethernet	This displays if the physical port is Power over Ethernet (PoE) enabled.

Related Commands

Command	Description
ap enet-link-profile	This command configures an AP Ethernet link profile.

Command History

Release	Modification
ArubaOS 8.3.0.0	A new row 802.3bz displays if the standard is enabled or disabled for an AP.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap essid

```
show ap essid
```

Description

This command shows an ESSID summary for the controller, including the number of APs and clients associated with each ESSID.

Examples

The following example shows statistics for four configured ESSIDs (For versions prior to ArubaOS 8.9.0.0).

```
(host) [mynode] #show ap essid
ESSID Summary
-----
ESSID          APs  Clients  VLAN(s)  Encryption
-----
vocera  21   0         66      WPA2 PSK AES
voip    23   52        66,64   WPA2 8021X AES
guest   49   6         63      Open
wpa2    26   88        65,64   WPA2 8021X AES
Num ESSID:4
```

The following example shows statistics for two configured ESSIDs (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] #show ap essid
ESSID Summary
-----
ESSID          APs  MBSSID Tx BSS  Clients  VLAN(s)  Encryption
-----
8@hbm-635-psk  1    1             0         1         WPA3 SAE AES
9@hbm-535-rtp  1    0             0         1         WPA2 PSK AES
Num ESSID:2
```

The output of this command includes the following information:

Parameter	Description
ESSID	An Extended Service Set Identifier (ESSID) is the identifying name of an 802.11 wireless network.
APs	Number of APs associated with the ESSID.

Parameter	Description
MBSSID Tx BSS (ArubaOS 8.9.0.0 or later versions)	Number of APs that have the specific BSSID or virtual AP as the transmitted virtual AP.
Clients	Number of clients associated with the ESSID.
VLAN(s)	VLAN IDs of the VLANs for the ESSID.
Encryption	The layer-2 authentication and encryption used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the MBSSID Tx BSS parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap est-status

```
show ap est-status ap-name <ap-name> | ip-addr <ip-addr>
```

Description

Shows the EST status of APs terminated on the controller.

Parameter	Description
ap-name <ap-name>	Show data for a specific AP by entering the name of the AP for which you want to display information.
ip-addr <ip-addr>	Show data for an AP with the specified IP address.

Example

The following example shows the EST status of an AP:

```
(host) [mynode] #show ap est-status ap-name b4:5d:50:ce:18:36
Server Host           : 10.15.100.142
Server Port          : 443
EST Status            : Enabled
Enrollment Status    : Enrolled
Local time           : Thu Sep 12 15:25:49 2019 IST
Cert beg             : Thu Sep 12 15:05:59 2019 IST
Cert end             : Sat Oct 12 15:35:59 2019 IST
Reenrollment due     : Sat Oct 5 03:28:29 2019 IST
Reenrolled           : No
Reenroll periodic timer : Running, 604815 Sec
```

Related Command

Command	Description
est	This command configures an EST profile on the controller.

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable / Config mode on Mobility Conductor.

show ap get-crash-dumps-status

```
show ap get-crash-dumps-status ap-name <apname>
```

Description

This command displays the status of the crash dump file transfers to a controller.

Example

The following output is displayed when crash dumps are successfully transferred:

```
Starting command execution, Time: Wed Apr 29 14:59:42 2020

Uploading to controller 10.3.51.100
- nssimem.myap555.0000.2020-04-26_18-52-45.gz, Status: Success(3)
- q6mem.myap555.0000.2020-04-26_18-52-45.gz, Status: Success(3)
- nssddr.myap555.0000.2020-04-26_18-52-45.gz, Status: Success(3)
- imem.myap555.0000.2020-04-26_18-52-45.gz, Status: Success(3)
Finished Command execution

All transfers Successful. Use 'tar crash' to create a crash.tar which can
be extracted via the usual methods from the controller flash directory
```

The following output is displayed when no crash dumps are present in the AP's flash memory:

```
No crash dumps found stored in the AP flash
```

Related Commands

Command	Description
ap get-crash-dumps	This command allows AP coredump files to be transferred to the controller flash memory on demand from the AP flash memory.

Command History

Release	Modification
ArubaOS 8.7.0.0	This command is introduced.

Command Information

Platforms	License	Mode
AP-534, AP-535, AP-555 access points	Base operating system.	Enable or config mode on managed devices.

show ap general-profile

```
show ap general-profile
```

Description

This command shows the general profile of an AP.

Example

The following example shows the general profile of an AP:

```
(host) [mynode] #show ap general-profile

ap general-profile
-----
Parameter                                     Value      Set
-----
Enable AP State Periodic Sync                 Enabled
AP State sync interval in minutes (5 - 1440 mins(24 hours)) 5 minutes
```

Related Commands

Command	Description
ap general-profile	This command configures the general profile of an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap global

```
show ap global ace-table [ace <acenum>| acl <aclnum> | all][acl-table]
```

Description

This command shows the central database of an AP.

Parameter	Description
ace-table	Show ACE table from AP's central database .
ace <acenum>	Dump single ace entry.
acl <aclnum>	Dump ACE entries for a single ACL.
all	Dump all ACE entries.
acl-table	Show ACL table of STM.

Example

The following example shows the ACL table of STM:

```
(host) [mynode] #show ap global acl-table

STM ACL Table
-----
ACL  Type      ACE Index  Ace Count  Name
---  ---
1    session    7680      1          global-sacl
2    role       8132      33         logon
3    session    7863      12         validuser
4    session    7680      1          sdn-acl
5    session    7684      1          uplink-lb-cfg-racl
6    session    7685      1          uplink-lb-sys-racl
7    role       7909      12         guest
8    session    7680      1          apprf-guest-sacl
9    role       7921      35         ap-role
10   role       7680      1          stateful-dot1x
11   session    7680      1          apprf-stateful-dot1x-sacl
12   role       8104      28         guest-logon
13   role       8892      37         sys-ap-role
14   session    7686      20         sys-control
15   session    8874      18         sys-ap-acl
16   session    8167      3          stateful-dot1x
17   session    7821      4          ap-uplink-acl
18   session    7724      1          master/ conductor -boc-traffic
19   session    7680      1          name
20   session    7725      2          validuserethacl
```

21	session	7680	1	name2
22	session	7727	2	etherypte
23	session	7729	3	wificalling-block
24	session	7732	11	v6-control
25	session	7743	2	dns-acl
26	session	7745	3	svp-acl
27	session	7748	2	v6-http-acl
28	session	7750	2	srcnat
29	session	7680	1	apprf-authenticated-sacl
30	session	7680	1	voip-applications-acl
31	session	7752	5	allow-diskservices
32	session	7757	2	dhcp-acl
33	session	7759	6	vpnlogon
34	session	7765	2	v6-icmp-acl
35	session	7767	2	wificalling-acl
36	session	7769	2	tftp-acl
37	session	8097	7	captiveportal
38	session	7778	6	vmware-acl
39	session	7784	3	skype4b-acl
40	session	7787	7	ap-acl
41	session	7794	2	v6-allowall
42	session	7680	1	apprf-default-via-role-sacl
43	session	7796	3	jabber-acl
44	session	7680	1	apprf-default-vpn-role-sacl
45	session	7799	12	control
46	session	7811	8	logon-control
47	session	7819	2	v6-dns-acl
48	session	7825	2	noe-acl
49	session	7827	2	v6-https-acl
50	session	7829	7	v6-ap-acl
51	session	7680	1	apprf-voice-sacl
52	session	7836	2	https-acl
53	session	7838	2	skinny-acl
54	session	7840	2	vocera-acl
55	session	7842	2	http-acl
56	session	7844	7	captiveportal6
57	session	7851	4	allow-printservices
58	session	7855	2	ra-guard
59	session	7857	3	citrix-acl
60	session	7860	3	allowall
61	session	8165	2	cplogout
62	session	7877	3	sip-acl
63	session	7880	8	v6-logon-control
64	session	7888	2	icmp-acl
65	session	7890	2	v6-dhcp-acl
66	session	7892	3	h323-acl
67	role	7895	4	default-via-role
68	role	7899	5	default-vpn-role
69	role	7904	5	authenticated
70	role	8075	22	voice

Related Command

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap gps

```

advanced
  ap-name
  ip-addr
  ip6-addr
summary
  ap-name
  ip-addr
  ip6-addr

```

Description

This command displays the status of GPS profile of an AP.

Parameter	Description
advanced	Display the raw information of the GPS. NOTE: This parameter is only used for advanced debugging and should only be issued under the direct supervision of Aruba technical support.
ap-name	Display the raw GPS information of an AP specified by its name.
ip-addr	Display the raw GPS information of an AP specified by its IP address.

Parameter	Description
ip6-addr	Display the raw GPS information of an AP specified by its IPv6 address.
summary	Display the summary information of the GPS profile.
ap-name	Display the summary GPS information of an AP specified by its name.
ip-addr	Display the summary GPS information of an AP specified by its IP address.
ip6-addr	Display the summary GPS information of an AP specified by its IPv6 address.

Example

The output of the `show ap gps summary` command displays the summary of the GPS profile in an AP with name AP635.

```
(host) #show ap gps summary ap-name AP635

GPS Information
-----
Type      Position(Latitude, Longitude)  Altitude
-----
$GNRMC    39.4777853, 116.1905834          N/A
$GNGGA    39.4777853, 116.1905834          40.7 M
$GNGLL    39.4777853, 116.1905834          N/A
```

Related Commands

Command	Description
gps	Displays the status of the GPS profile.

Command History

Version	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap greenap

```
show ap greenap
amon pending-ap {all | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
counters{ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr> | wired-mac
<wired-mac>}
request pending-ap {all | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command displays all the pending APs in the per-md list, sends the AP_INFO AMON message for a particular AP, and track Green AP related counters.

Parameter	Description
amon	AMON message. When AP is in deep-sleep mode, the managed device sends the AP_INFO AMON message for a particular AP. NOTE: The amon command can only be run in the managed device
pending-ap	Displays the pending AP list.
all	Displays the pending AP list for the managed device.
ip-addr	Displays the pending AP list for a particular IP address of the managed device.
ip6-addr	Displays the pending AP list for a particular IPv6 address of the managed device.
counters	Displays all the counters for Green AP. This command is used to track green AP related counters, for example, how many deep-sleep or wake-up requests are received from Netinsight and how many requests are dropped, and so on.
ap-name	Displays the counters for a particular AP name.
ip-addr	Displays the counters for a particular IP address of the managed device.
ip6-addr	Displays the counters for a particular IPv6 address of the managed device.
request	Displays the power-save or wakeup requests for a Green AP. This command is used to display all the pending APs in the per-md list.

Example

The following command helps in debugging and tracking all the requests using counters:

```
show ap greenap counters ap-name <ap-name>
Counters for greenap
-----
Item                                     Value
----                                     -
Received deep-sleep requests            76
Received wake-up requests               14
Received agent-wake-up requests         3
Listed deep-sleep requests              20
Listed wake-up requests                 1
Listed agent-wake-up requests           3
Forwarded deep-sleep requests           20
Forwarded wake-up requests              1
Forwarded agent-wake-up requests        3
Acks sent for deep-sleep                 0
Acks sent for wake-up                   0
Acks sent for agent-wake-up             0
Acked deep-sleep requests               20
Acked wake-up requests                  1
Acked agent-wake-up requests            3
ACCEPT                                  0
PRELOAD                                  0
UPGRADE                                  0
PROVISION                                0
...
...
...
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor and managed device.

show ap he-rates

```
show ap he-rates bssid <bssid>
```

Description

This command shows high-efficiency rate information for a BSS.

Parameter	Description
bssid <bssid>	Show data for a specific BSSID on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The output of this command shows high-efficiency rates for each supported MCS value.

```
(host) [mynode] #show ap he-rates bssid 00:12:6d:03:1c:f1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap ht-rates

```
show ap ht-rates bssid <bssid>
```

Description

This command shows high-throughput rate information for a BSS.

Parameter	Description
bssid <bssid>	Show data for a specific BSSID on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The output of this command shows high-throughput rates for each supported MCS value. These values are applicable to high-throughput (802.11n-capable) APs only.

```
(host) [mynode] #show ap ht-rates bssid 00:1a:1e:1e:5a:10
AP "AL12" Radio 0 BSSID 00:1a:1e:1e:5a:10 High-throughput Rates (Mbps)
-----
MCS  Streams  20 MHz  40 MHz  40 MHz SGI
----  -
0    1          6.5    13.5    15.0
1    1          13.0   27.0    30.0
2    1          19.5   40.5    45.0
3    1          26.0   54.0    60.0
4    1          39.0   81.0    90.0
5    1          52.0  108.0   120.0
6    1          58.5  121.5   135.0
7    1          65.0  135.0   150.0
8    2          13.0   27.0    30.0
9    2          26.0   54.0    60.0
10   2          39.0   81.0    90.0
11   2          52.0  108.0   120.0
12   2          78.0  162.0   180.0
13   2         104.0  216.0   240.0
14   2         117.0  243.0   270.0
15   2         130.0  270.0   300.0
```

The output of this command includes the following information:

Parameter	Description
MCS	A Modulation Coding Scheme (MCS) values supported on this high-throughput SSID.

Parameter	Description
Streams	Number of spatial streams used by the MCS index value.
20 MHz	802.11n data rates for the MCS for 20 Mhz transmissions.
40 MHz	802.11n data rates for the MCS for 40 Mhz transmissions.
40 MHz SGI	802.11n data rates for the MCS for 40 Mhz transmissions using a short guard interval.

Related Commands

Command	Description
show ap vht-rates	Show very-high-throughput rate information for a basic service set (BSS).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.


```

AP Name          AP Group      AP IP      AP Type  Preload State  Start
Time            End Time      Failure Count Failure Reason
-----
6c:f3:7f:c3:a6:56 SecureJack  10.3.90.14  135      Preloaded      2013-11-
05 15:38:50    2013-11-05 15:39:58  0

```

(host) #show ap image-preload status list

```

AP Image Preload AP Status
-----
AP Name          AP Group      AP IP      AP Type  Preload State  Start
Time            End Time      Failure Count Failure Reason
-----
6c:f3:7f:c3:a6:56 SecureJack  10.3.90.14  135      Preloaded      2013-11-
05 15:38:50    2013-11-05 15:39:58  0

```

(host) #show ap image-preload status summary

```

AP Image Preload Parameters
-----
Item              Value
-----
Status            Active
Mode              All APs
Partition         0
Build             40740
Max Simultaneous Downloads 512
Start Time        2013-11-05 15:38:50
AP Image Preload AP Status Summary
-----
AP Image Preload State  Count
-----
Preloaded               1
TOTAL                   1

```

The output of this command includes the following information:

Parameter	Description
AP Image Preload Parameters	Shows if this feature has been enabled (has an active status) or is disabled (has an inactive status).
AP Image Preload AP Status Summary	<p>These two columns list the different possible preload states for APs eligible to preload a new software image, and the total number of APs in each state.</p> <ul style="list-style-type: none"> ■ Preloaded: Number of APs that have finished preloaded a new software image. ■ Preloading: Number of APs that are currently downloading the new image.

Parameter	Description
	<ul style="list-style-type: none"> ■ Waiting: Number of APs that are waiting to start preloading the new image from the controller.
AP Image Preload AP Status	This section displays the following details for each preload attempt.
AP Name	Name of an AP eligible to preload a new software image.
AP Group	AP group of an AP eligible to preload a new software image.
AP IP	IP address of the AP.
AP Type	AP model type.
Preload State	<p>Current state of the AP's preload attempt</p> <ul style="list-style-type: none"> ■ Preloaded: The AP is finished preloading a new software image. ■ Preloading: The AP is currently downloading the new image. ■ Waiting: The AP is waiting to start preloading the new image from the controller.
Start Time	Time the AP starting preloading an image.
End Time	Time the AP completed the image preload.
Failure Count	Number of times that the AP failed to preload the new image.
Failure Reason	In the event of an image preload failure, this column will display the reason that the image download failed.

Related Commands

Command	Description
show ap image version	Display an AP's image version information.

Command History

Release	Modification
ArubaOS8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor or managed devices.

show ap image version

```
show ap image version [ap-name <ap-name>|ip-addr <ip-addr>]
```

Description

This command shows an AP's image version information. By default, this command displays image version information for all APs associated with the controller. To view image version information for a single AP, specify an AP using the `ap-name` or `ip-addr` parameters.

Parameter	Description
<code>ap-name <ap-name></code>	View image version information for an AP with a specific name.
<code>ip-addr <ip-addr></code>	View image version information for an AP with a specific IP address. Enter the address of the AP in dotted-decimal format.

Example

The output in the example below shows the current running image version as well as the image version stored in the controller's flash memory.

```
(host) [mynode] #show ap image version ip-addr 192.0.2.45
Access Points Image Version
-----
AP                               Running Image Version String
--                               -----
192.0.2.45                       6.4.0.0 Wed Nov 27 10:46:42 PDT 2013

Flash Image Version String      Matches   Num Matches
-----
6.4.0.0 Wed Nov 27 10:46:42 PDT 2013  Yes      3

Num Mismatches   Bad Checksums   Image Load Status
-----
0                -----          Done
```

The output of this command includes the following information:

Parameter	Description
AP	Name or IP address of an AP.

Parameter	Description
Running Image Version String	String identifying the number of the image version currently running on the AP, as well as the date on which that version was created.
Flash Image Version String	String identifying the number of the image version in the AP's flash memory, as well as the date on which that version was created.
Matches	If yes , the running image version matches the image version currently in the AP's flash memory. If no , the two image versions do not match.
Num Matches	Number of times the running image version matched the flash image version after a reboot.
Num Mismatches	Number of times the running image version did not match the flash image version after a reboot. If the images do not match, the AP will upgrade to the flash image.
Bad Checksums	Number of bad checksum calculations due to an invalid or corrupted image file.
Image Load Status	Current status of the AP following an upgrade. <ul style="list-style-type: none"> ■ Done: This status indicates that the controller reset after the upgrade was performed, or the upgrade was performed after the AP first registered with the controller. ■ Completed: The AP was updated after it was registered to the controller, and after the controller's last reset. If AP shows a status of completed, it will also display the time it took it update that AP. ■ In progress: The AP is currently updating its image.

Related Commands

Command	Description
show ap image-preload status	This command displays the list of APs that will preload a new version of software from a controller with the AP preload feature activated.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap ip health-check

```
show ap ip health-check {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows health of an access point.

Parameter	Description
ap-name <ap-name>	Shows health of an access point specified by AP name.
ip-addr <ip-addr>	Shows health of an access point specified by IP address.
ip6-addr <ip6-addr>	Shows health of an access point specified by IPv6 address.

Example

Access the CLI and use the following command to show health of an access point with IP address 192.0.2.1:

```
(host) [mynode] #show ap ip health-check ip-addr 192.0.2.1

AP Health-Check Status
-----
Interval  Probe IP  Avg RTT(in ms)  Total_TX_Probes  Total_RX_Probes  Total_
Packet Loss
-----
-----
```

Related Commands

Command	Description
show ip health-check	This command displays the health-check status of the uplink interfaces of a branch office managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap-lacp-striping-ip

show ap-lacp-striping-ip

Description

Profile to enable/disable AP LACP feature and to specify GRE striping IP to LMS IP mapping.

Example

```
(host) [mynode] #show ap-lacp-striping-ip
AP LACP LMS map information
-----
Parameter          Value
-----
AP LACP Striping IP Enabled
GRE Striping IP    2.2.2.2 LMS 3.3.3.3
GRE Striping IP    4.4.4.4 LMS 5.5.5.5
GRE Striping IP    10.65.30.50 LMS 10.65.30.60
```

Related Commands

Command	Description
ap-lacp-striping-ip	This command defines an AP LACP LMS map information profile that maps a GRE striping IP address to an existing LMS-IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap license-usage

show ap license-usage

Description

This command shows AP license usage information.

Examples

The output of the command below shows that controller has 13 associated campus APs using licenses, with 3 unused campus AP licenses remaining.

```
(host) [mynode] #show ap license-usage

AP Licenses
-----
Type                Number
-----
AP Licenses         512
MM Licenses          500
MC-VA Licenses      0
Controller License  True
Overall AP License Limit 0
AP Usage [Note: THIS CONTROLLER DOES NOT TERMINATE ANY AP]
-----
Type                Count
-----
Active CAPs         0
Active RAPs         0
Remote-node APs     0
Tunneled nodes     0
Total APs           0
Remaining AP Capacity
-----
Type  Number
-----
CAPs  0
RAPs  0
```

The output of this command includes the following information:

Parameter	Description
AP Licenses	Number of AP licenses currently available on the managed device.
RF Protect Licenses	Number of RF Protect licenses currently available on the managed device.

Parameter	Description
PEF Licenses	Number of PEF licenses currently available on the managed device.
Overall AP Licenses	Total number of APs supported by licenses on the managed device.
CAPs	Number of campus APs currently using a license on the managed device.
RAPs	Number of remote APs currently using a license on the managed device.
Remote-Node APs	Number of APs currently using a license on the managed device.
Tunneled Nodes	Number of tunneled nodes currently using a license on the managed device.
CAPs	Number of unused campus APs licenses remaining on the managed device.
RAPs	Number of unused remote APs licenses remaining on the managed device.

Related Commands

Command	Description
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap lldp

```
show ap lldp [<profile>]
```

Description

Display a list of LLDP-MED Network Policy profiles, or display the current configuration settings of an individual profile.

Parameter	Description
<profile>	Specify a LLDP profile name to view configuration settings for that profile.

Examples

The following example lists all LLDP profiles. The References column lists the number of other profiles with references to that LLDP-MED Network policy profile, and the ProfileStatus column indicates whether the profile is predefined.

The output of the command below shows that the controller has two LLDP profiles.

```
(host) #show ap lldp med-network-policy-profile
AP LLDP Profile List
-----
Name      References  Profile Status
-----
default   0
video     2
Total:2
The following command displays configuration details for the LLDP profile
named default.

(host) [mynode] #show ap lldp med-network-policy-profile video
AP LLDP Profile "new"
-----
Parameter                               Value
-----
PDU transmission                         Enabled
Reception of LLDP PDUs                  Enabled
Transmit interval (seconds)              30
Transmit hold multiplier                  4
Optional TLVs                            port-description system-description system-
name capabilities management-address
802.1 TLVs                               port-vlan vlan-name
802.3 TLVs                               mac link-aggregation mfs power
LLDP-MED TLVs
LLDP-MED network policy profile         N/A
```

The output of this command includes the following information:

Parameter	Description
PDU transmission	Shows if LLDP PDU transmission is enabled on the AP.
Reception of LLDP PDUs	Shows if LLDP PDU reception is enabled on the AP.
Transmit interval (seconds)	The interval between LLDP TLV transmission seconds. The supported range is 1-3600 seconds and the default value is 30 seconds.
Transmit hold multiplier	This value is multiplied by the transmit interval to determine the number of seconds to cache learned LLDP information before that information is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then learned LLDP information will be cached for 4 x 30 seconds, or 120 seconds.
Optional TLVs	The AP sends the listed optional TLVs in LLDP PDUs.
802.1 TLVs	The AP sends the listed 802.1 TLVs in LLDP PDUs. By default, the AP will send all 802.1 TLVs.
802.3 TLVs	The AP sends the listed 802.3 TLVs in LLDP PDUs. By default, the AP will send all 802.3 TLVs.
LLDP-MED TLVs	Lists the LLDP-MED TLVs the AP will send in LLDP PDUs. By default, the AP will not send any LLDP-MED TLVs
LLDP-MED network policy profile	Specifies the LLDP MED Network Policy profile to be associated with this LLDP profile.

Related Commands

Command	Description
ap lldp profile	This command defines an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap lldp counters

```
show ap lldp counters
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr (ipv6-addr)
```

Description

This command shows LLDP counters for a specific AP, or all APs sending or receiving LLDP Protocol Data Units (PDUs).

Parameter	Description
ap-name <ap-name>	Show counter statistics for an AP with a specific name.
ip-addr <ip-addr>	View counter statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.
ip6-addr <ip-addr>	View counter statistics for an AP with a specific IPv6 address.

Examples

The output of the command below shows LLDP counter information for two interfaces.

```
(host) [mynode] #show ap lldp counters
AP LLDP Counters (Updated every 60 seconds)
-----
AP          Interface  Received  Unknown TLVs  Malformed  Overflow
Transmitted
--          -
-----
00:1a:1e:ce:fb:bf bond0      0          0              0          0
68159
00:24:6c:c0:00:86 bond0      0          0              0          0
68153
```

The output of this command includes the following information:

Parameter	Description
AP	Name of the AP sending or receiving LLDP PDUs.
Interface	Name of the AP interface sending or receiving LLDP PDUs.
Received	Number of packets received on the specified interface.

Parameter	Description
Unknown TLVs	Number of LLDP Protocol Data Units (PDUs) with an unknown type-length-value (TLV).
Number of Malformed packets	Number of malformed packets received on that interface.
Overflow	Number of times that an LLDP neighbor could not be added to the neighbor table (there is a limit of 8 per port).
Transmitted	Number of packets transmitted from that interface.

Related Commands

Command	Description
ap lldp profile	This defines an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap lldp med-network-policy-profile

show ap lldp med-network-policy-profile [<profile>]

Description

This command shows a list of LLDP-MED Network Policy profiles, or display the current configuration settings of an individual profile. The LLDP-MED Network policy profile allows you to configure an extension to LLDP that supports interoperability between VoIP devices and other networking clients. LLDP-MED network policy discovery lets end-points and network devices advertise their VLAN IDs (e.g. voice VLAN), priority levels, and DSCP values. allows you to define a set of provisioning parameters to an AP group.

Issue this command without the **<profile-name>** option to display the entire LLDP-MED Network policy profile list, including profile status and the number of references to each profile. Include a profile name to display the configuration settings for that profile.

Parameter	Description
<profile>	Specify a LLDP-MED Network Policy profile name to view configuration settings for that profile.

Examples

The following example lists all LLDP-MED Network policy profile profiles. The **References** column lists the number of other profiles with references to that LLDP-MED Network policy profile, and the **Profile Status** column indicates whether the profile is predefined.

The output of the command below shows that the controller has three LLDP-MED network profiles.

```
(host) [mynode] #show ap lldp med-network-policy-profile

AP LLDP-MED Network Policy Profile List
-----
Name      References  Profile Status
----      -
default   0
video     2
voice     1
Total:2
The following command displays configuration details for the LLDP-MED
Network Policy profile named video.

(host) #show ap lldp med-network-policy-profile video
AP LLDP-MED Network Policy Profile "default"
-----
Parameter                                     Value
```

```

-----
LLDP-MED application type                streaming-video
LLDP-MED application VLAN                16
LLDP-MED application VLAN tagging        Tagged
LLDP-MED application Layer-2 priority    0
LLDP-MED application Differentiated Services Code Point 0

```

The output of this command includes the following information:

Parameter	Description
LLDP-MED application type	<p>Type of application that this profile manages. This profile supports the following options:</p> <ul style="list-style-type: none"> ■ guest-voice: The AP services a separate voice network for guest users and visitors. ■ guest-voice-signaling: The AP is part of a network that requires a different policy for guest voice signaling than for guest voice media. Do not use this application type if both the same network policies apply to both guest voice and guest voice signaling traffic. ■ softphone-voice : The AP supports voice services using softphone software applications on devices such as PCs or laptops. ■ streaming-video: T The AP supports broadcast or multicast video or other streaming video services that require specific network policy treatment. This application type is not recommended for video applications that rely on TCP with buffering. ■ video-conferencing: T The AP supports video conferencing equipment that provides real-time,

Parameter	Description
	<p>interactive video/audio services.</p> <ul style="list-style-type: none"> ■ video-signaling: T The AP is part of a network that requires a different policy for video signaling than for the video media. Do not use this application type if both the same network policies apply to both video and video signaling traffic. ■ voice: The AP services IP telephones and other appliances that support interactive voice services. This is the default application type. ■ voice-signaling: The AP is part of a network that requires a different policy for voice signaling than for the voice media. Do not use this application type if both the same network policies apply to both voice and voice signaling traffic.
LLDP-MED application VLAN	Indicates the VLAN ID (0-4094) or VLAN name of the VLAN used by the application.
LLDP-MED application VLAN tagging	<p>Indicates if the policy applies to a to a VLAN that is tagged with a VLAN ID or untagged. The default value is untagged.</p> <p>NOTE: When an LLDP-MED network policy is defined for use with an untagged VLAN, then the L2 priority field is ignored and only the DSCP value is used.</p>

Parameter	Description
LLDP-MED application Layer-2 priority	Displays a configured 802.1p priority level for the specified application type, where 0 is the lowest priority level and 7 is the highest priority.
LLDP-MED application Differentiated Services Code Point	Displays a configured Differentiated Services Code Point (DSCP) priority value for the specified application type, where 0 is the lowest priority level and 63 is the highest priority.

Related Commands

Command	Description
ap lldp med-network-policy-profile	This command defines an LLDP MED network policy profile that defines DSCP values and L2 priority levels for a voice or video application.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap lldp neighbors

```
show ap lldp neighbors
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr (ipv6-addr)
```

Description

This command shows LLDP neighbors for a specific AP, or all APs sending or receiving LLDP Protocol Data Units (PDUs). The LLDP protocol allows switches, routers, and WLAN access points to advertise information about themselves such as identity, capabilities, and neighbors to other nodes on the network. Use this command to display information about the AP's LLDP peers.

By default, this command displays LLDP neighbors for the entire list of LLDP interfaces. Include a the name of IP address of an AP to display neighbor information only for that one device.

Parameter	Description
ap-name <ap-name>	Show LLDP neighbor statistics for an AP with a specific name.
ip-addr <ip-addr>	View LLDP neighbor statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.
ip6-addr <ip-addr>	View LLDP neighbor statistics for an AP with a specific IPv6 address.

Examples

The output of the command below shows the LLDP neighbor list for an AP named **ap12**.

```
(host) [mynode] #show ap lldp neighbors ap-name ap12
AP LLDP Neighbors (Updated every 60 seconds)
-----
AP Interface Neighbor Chassis Name/ID Port Name/ID Mgmt. Address
Capabilities
--
-----
uc bond0 0 d8:c7:c8:c4:4f:4e bond0 10.3.44.193
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
```

The output of this command includes the following information:

Parameter	Description
AP	Name of the LLDP neighbor
Interface	Interface on the AP sending or receiving LLDP PDUs.
Neighbor	LLDP neighbor number
Chassis Name/ID	The name of the LLDP neighbor AP
Port Name/ID	Port name or ID if the interface sending LLDP PDUs.
Mgmt. Address	Management address of the LLDP neighbor
Capabilities	This data column can list any of the following data codes to indicate LLDP neighbor capabilities. <ul style="list-style-type: none"> ■ R: Router ■ B: Bridge ■ A: Access Point ■ P: Phone ■ O: Other

Related Commands

Command	Description
ap lldp profile	This command defines an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap load-balancing

```
show ap load balancing
```

Description

This command shows the load-balancing information for each AP with load balancing enabled.

Examples

The output of the command in the example below shows details for a single AP enabled with the load-balancing feature.

```
(host) [mynode] #show ap load-balancing
Load Balance Enabled Access Point Table
-----
bss          ess          name    s/p  ip          phy    chan  cur-cl  util (kbps)
---          ---          ----    --  --          ---    ----  -
00:0b:86:cc:8e:4e Wireless_1  mp22    2/24  10.3.148.12 a-HT   413   3       14
```

The output of this command includes the following information:

Column	Description
BSS	The BSS Identifier for the AP. This is usually the APs MAC address.
ESS	The ESS Identifier is the user-defined name of an 802.11 wireless network.
s/p	The controller slot and port used by the AP, in the format <slot>/<module>/<port>.
ip	IP address of the AP.
phy (For versions prior to ArubaOS 8.9.0.0)	Displays one of the following 802.11 radio types: <ul style="list-style-type: none">■ a■ a-HT (high-throughput)■ g■ g-HT (high-throughput)
Phy-type (ArubaOS 8.9.0.0 or later versions)	Displays one of the following 802.11 radio types: <ul style="list-style-type: none">■ 2.4GHz■ 5GHz■ 6GHz

Column	Description
chan	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the AP's regulatory domain (country).
cur-cl	Current number of clients on the AP.
util (kbps)	Current bandwidth utilization, in kbps.

Related Commands

Command	Description
uplink	This manages and configures the uplink network connection.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> Replaced <code>phy</code> with <code>Phy-type</code> parameter. Replaced a and g with 5GHz and 2.4GHz values. Introduced 6GHz value for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

```
show ap mesh-accesslist-profile <name>
```

Description

This command displays the details of the mesh access list profile.

Example

The following command displays the details of a mesh access list profile:

```
(host) [mynode] #show ap mesh-accesslist-profile guest
-----
Parameter  Value
-----
AP name    AP-505
Type       allow
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show ap mesh

```
show ap mesh
  active
  debug
  monitor
  neighbors
  tech-support
  topology
```

Description

This command shows all information for a mesh AP. Click parameter links to view the corresponding show commands.

Parameter	Description
active	Shows mesh cluster APs currently registered on the switch.
debug	Shows mesh debugging information.
monitor	Shows mesh monitor information.
neighbors	Shows all mesh neighbors.
tech-support	Shows all information for an AP.
topology	Shows mesh tree topology.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the secure enterprise mesh solution for outdoor APs require the Outdoor Mesh license.	Enable or Config mode on managed devices.

show ap mesh active

```
show ap mesh active [<mesh-cluster>|{page <page>}|{start <start>}]
```

Description

This command shows active mesh cluster APs currently registered on this Mobility Conductor.

Parameter	Description
<mesh-cluster>	Name of a mesh cluster profile.
page <page>	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
start <start>	Start displaying the index of mesh APs at a chosen index number by entering the index number of the AP at which command output should start.

Example

The following example displays a list of all active mesh points and mesh portals (For versions prior to ArubaOS 8.9.0.0).

```
(host)[mynode] #show ap mesh active
Mesh Cluster Name: mesh-515
-----
Name      Group      IP Address      AP Type  Uptime          Mesh Role  MTU
Enet Ports Parent #Children Radio0 Band/Ch/EIRP/MaxEIRP Radio1
Band/Ch/EIRP/MaxEIRP Radio2 Band/Ch/EIRP/MaxEIRP
-----
-----
-----
ap225 mesh-515 172.16.1.6      225      2d:17h:40m:1s  Point
Off/Off  ap505 1
802.11g/1/15.0/25.0
ap345 mesh-515 172.16.1.4      345      2d:14h:25m:8s  Point
Off/Off  ap505 0
802.11a/36E/15.0/25.2
ap375 mesh-515 172.16.1.115    375      2d:17h:36m:26s Point
Off/Off  ap225 0
802.11g/1/15.0/29.7
ap505 mesh-515 172.16.1.108    505      2d:13h:56m:36s Portal  1578 -
-        2          802.11a/36E/15.0/29.5

Total APs :4
```


Starting from ArubaOS 8.7.0.0, the **show ap mesh active** command displays the above output only when mesh enabled radios are present. Else, the output will be displayed as following:

```
(host) [ mynode] #show ap mesh active
Total APs :5
```

The following example displays a list of all active mesh points and mesh portals for AP-635 access point (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] #show ap mesh active

Mesh Cluster Name: jiajunname
-----
Name      Group   IP Address   AP Type  Uptime      Mesh Role  MTU   Enet
Ports    Parent  #Children   Radio0  Band/Ch/EIRP/MaxEIRP  Radio1
Band/Ch/EIRP/MaxEIRP  Radio2  Band/Ch/EIRP/MaxEIRP
-----  -----  -----  -----  -----  -----  ---  ---
-----  -----  -----  -----  -----  -----  ---  ---
ap635-3  mesh6xx 10.10.117.253 635      22h:45m:36s Portal     1500  -
/Off      -        1
          6GHz/169S/20.0/21.5
ap635-4  mesh6xx 10.10.117.252 635      22h:33m:46s Point
Off/Bridge ap635-3 0
          6GHz/169S/20.0/21.5

Total APs :2
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.
Group	AP group which includes the specified AP.
IP Address	IP address of the AP.
AP type	The AP model type.
Uptime	Number of hours, minutes and seconds since the last Mobility Conductor reboot or bootstrap, in the format <i>hours:minutes:seconds</i> .
Mesh Role	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
MTU	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.

Column	Description
Enet Ports	Shows one of the following current modes of each wired interface: <ul style="list-style-type: none"> ■ Bridge: 802.11 frames are bridged into the local Ethernet LAN. ■ Tunnel: 802.11 frames are tunneled to the Mobility Conductor using GRE. ■ Split-tunnel: 802.11 frames are either bridged into the local Ethernet LAN or tunneled to the Mobility Conductor, depending upon their destination. ■ Off: Interface is not available for serving clients. If an AP has only one wired interface, the output of this command will display a dash (-) for the unavailable port.
Parent	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal. Mesh portals will display a dash (-).
#Children	If the AP is operating as a mesh portal, this parameter shows the number of mesh point children associated with that mesh portal.
Band/Ch/EIRP/MaxEIRP	The RF band in which the AP should operate (a or g)/radio channel used by the AP/current EIRP /maximum EIRP. <p>NOTE: For Wi-Fi 6E APs in ArubaOS 8.9.0.0 or later versions, the RF band displays one of the following values:</p> <ul style="list-style-type: none"> ■ 2.4 GHz ■ 5 GHz ■ 6 GHz

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the RF bands as 2.4 GHz , 5 GHz , or 6 GHz .
ArubaOS 8.7.0.0	This command displays a detailed output of all parameters only if mesh -enabled radios are configured.

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the secure enterprise mesh solution for outdoor APs require the Outdoor Mesh license.	Enable or Config mode on managed devices.

show ap mesh debug

```
show ap mesh debug
  counters
  current-cluster
  forwarding-table
  hostapd-log
  link-table
  meshd-log
  provisioned-clusters
  session-log
  status
```

Description

This command shows mesh debugging information of APs. Click parameter links to view the corresponding show commands.

Parameter	Description
counters	Shows statistics for a mesh node.
current-cluster	Shows mesh cluster profile currently used by a mesh node.
forwarding-table	Shows forwarding table of a MESH node.
hostapd-log	Shows debug log messages of hostapd process.
link-table	Shows link table of a mesh node.
meshd-log	Shows debug log messages of meshd process.
provisioned-clusters	Shows mesh cluster profiles provisioned on a mesh node.
session-log	Shows session log messages of meshd process.
status	Shows mesh internal status of a mesh node.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh debug counters

```
show ap mesh debug counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

This command shows counters statistics for a mesh node.

Parameter	Description
ap-name <ap-name>	Show counter statistics for an AP with a specific name.
bssid <bssid>	Show counter statistics for a specific BSSID on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	View counter statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.

Example

The example below shows the Mesh Packet Counters table for an AP named meshpoint1. The **Probe Resp**, **Assoc Req**, and **Assoc Resp** data columns show both the total number of counters and, in parenthesis, the number of requests or responses with high-throughput information elements (HE IEs).

```
(host) [mynode] #show ap mesh debug counters ap-name meshpoint1
Mesh Packet Counters
-----
Interface  Echo Sent  Echo Recv  Probe Req  Probe Resp  Assoc Req  Assoc
Resp  Assoc Fail  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----  -----
Link up/down  Resel.  Switch  Other
-----  -----  -----  -----
Parent        68865    68755    24        8 (8 HT)  3 (1 HT)  3 (1 HT)
  1
1              -        -        0
Child        68913    67373    6         8         2
  2              0        1         2         0        2618886

Received Packet Statistics: Total 2890717, Mgmt 2618946 (dropped non-mesh
0), Data 271771 (dropped unassociated 1)HT: pns=8 ans=1 pnr=0 ars=0 arr=1
anr=0

Recovery Profile Usage Counters
-----
Item                Value
----                -
Enter recovery mode  0
Exit recovery mode   0
```

```
Total connections to switch 0
Mesh loop-prevention Sequence No.:1256947
Mesh timer ticks:68930
```

The output of this command includes the following information:

Column	Description
Interface	Indicates whether the mesh interface connects to a Parent AP or a Child AP. Each row of data in the <i>Mesh Packet Counters</i> table shows counter values for an individual interface.
Echo Sent	Number of echo packets sent.
Echo Recv	Number of echo packets received.
Probe Req	Number of probe request packets sent from the interface specified in the Mesh-IF parameter.
Probe Resp	Number of probe response packets sent to the interface specified in the Interface parameter.
Assoc Req	Number of association request packets from the interface specified in the <i>Interface</i> parameter.
Assoc Resp	Number of association response packets from the interface specified in the Interface parameter. This number includes valid responses and fail responses.
Assoc Fail	Number of fail responses received from the interface specified in the Interface parameter.
Link up/down	Number of times the link up or link down state has changed.
Resel.	Number of times a mesh point attempted to reselect a different mesh portal.
Switch	Number of times a mesh point successfully switched to a different mesh portal.
Other Mgmt	Management frames of any type other than association and probe frames, either received on child interface, or sent on parent interface.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh debug current-cluster

```
show ap mesh debug current-cluster
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command shows the AP mesh debug information for the mesh cluster currently used by a mesh point or mesh portal.

Parameter	Description
ap-name <ap-name>	Shows AP mesh debug information for the specified AP name.
bssid <bssid>	Shows AP mesh debug information for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh debug information for the specified IP address.

Examples

The example shows the AP mesh debug information of an AP named **mp2**.

```
(host) [mynode] #show ap mesh debug current-cluster ap-name mp2

AP "mp2" Current Cluster Profile: default
-----
Item                Value
----                -
Cluster Name       smettu-mesh
RF Band            a
Encryption         opensystem
WPA Hexkey         N/A
WPA Passphrase     *****
```

The output of this command includes the following information:

Column	Description
Cluster Name	Name of the mesh cluster using this profile
RF band	The RF band in which the mesh point or mesh portal operates: <ul style="list-style-type: none">■ g = 2.4 GHz

Column	Description
	<ul style="list-style-type: none"> ■ a = 5 GHz
Encryption	Data encryption setting for the mesh cluster profile. <ul style="list-style-type: none"> ■ opensystem—No authentication and encryption. ■ wpa2-psk-aes—WPA2 with AES encryption using a preshared key.
WPA Hexkey	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
WPA Passphrase	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh debug forwarding-table

```
show ap mesh forwarding-table [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>]
```

Description

This command displays the forwarding table for a remote mesh point or remote mesh portal. This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with your mesh network.

Parameter	Description
ap-name <ap-name>	Show data for a remote mesh node with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for a remote mesh node with a specific IP address by entering its IP address in dotted-decimal format.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>bssid</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh debug hostapd-log

```
show ap mesh debug hostapd-log
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command shows the AP mesh debug log messages for the **hostapd** process. This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with the **hostapd** process or your mesh network.

Parameter	Description
ap-name <ap-name>	Shows AP mesh debug log messages for the specified AP name.
bssid <bssid>	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh debug log messages for the specified IP address.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh debug link-table

```
show ap mesh debug link-table [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>]
```

Description

This command shows the mesh link table for a remote mesh point or remote mesh portal. This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with your mesh network.

Parameter	Description
ap-name <ap-name>	Show data for a remote mesh node with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for a remote mesh node with a specific IP address by entering its IP address in dotted-decimal format.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh debug meshd-log

```
show ap mesh debug meshd-log {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} [<page>]
```

Description

Show the debug log messages for the **meshd** process. This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with the **meshd** process or your mesh network.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
<page>	Display page number 0, 1, or 2, where page 0 has the newest information and page 2 has the oldest. If this parameter is omitted, this command will display all meshd log information, oldest first.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh debug provisioned-clusters

```
show ap mesh debug provisioned-clusters
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command shows the cluster profiles provisioned on a mesh portal or mesh point.

Parameter	Description
ap-name <ap-name>	Shows AP mesh debug log messages for the specified AP name.
bssid <bssid>	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh debug log messages for the specified IP address.

Example

The example shows the statistics for the APs mesh cluster profile and recovery cluster profile on an AP mesh point named portal2.

```
(host) [mynode] #show ap mesh debug provisioned-clusters ap-name portal2

AP Portal Cluster Profile: mesh-cluster-profile
-----
Parameter      Value
-----
Cluster Name   sw-ad-GB32
RF Band        a
Encryption     opensystem
WPA Hexkey     N/A
WPA Passphrase *****

AP "Portal" Cluster Profile: Recovery Cluster Profile
-----
Item           Value
-----
Cluster Name   Recovery-ZF-xAP15z-g15VN
RF Band        a
Encryption     pa2-psk-aes
WPA Hexkey     *****
WPA Passphrase N/A
```

The output of this command displays the following information for the AP's mesh cluster profile and recovery cluster profiles:

Column	Description
Cluster Name	Name of the mesh cluster using this profile
RF band	The RF band in which the AP should operate: <ul style="list-style-type: none"> ■ g = 2.4 GHz ■ a = 5 GHz
Encryption	Data encryption setting for the mesh cluster profile. <ul style="list-style-type: none"> ■ opensystem—No authentication and encryption. ■ wpa2-psk-aes—WPA2 with AES encryption using a preshared key.
WPA Hexkey	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
WPA Passphrase	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh debug session-log

```
show ap mesh debug session-log
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command shows the session log messages of meshd process.

Parameter	Description
ap-name <ap-name>	Shows AP mesh debug log messages for the specified AP name.
bssid <bssid>	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh debug log messages for the specified IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh debug status

```
show ap mesh debug status
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command shows mesh internal status of a mesh node.

Parameter	Description
ap-name <ap-name>	Shows AP mesh debug log messages for the specified AP name.
bssid <bssid>	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh debug log messages for the specified IP address.

Example

The following example displays the mesh internal status of a mesh node:

```
(host) [mynode] #show ap mesh debug status ap-name ap225
Country-code: 0 ("US"), Outdoor: FALSE
Active Cluster: <mesha-psk2>, encrypted: TRUE, priority:1
All Available Clusters(1):
Cluster: <mesha-psk2>, encrypted: TRUE, priority: 1
Working RF Band: 2, RF Split 5G Range: 0
SM State: CONNECTED, Descendant Upgrading: FALSE, Portal Reachability: TRUE
Topology Adjust Scan: False, Scan Times: 0, Scan Interval: 1000s,
Portal ID: 84:d4:7e:e6:0b:01, Loop Protect Seq NO: 21529, Hop Count: 0, Path
Cost: 0, Portal MTU: 1578,
Metric Reselection State: Idle, Optimize Scan Tick: 21528, Reselection Tick:
21528, Switch Interval: 0, Switch Tick: 21528,
SAPD Pending: FALSE, Received Config: TRUE, Thermal Protect: FALSE, Reboot
Me: FALSE, Shutting Down: FALSE,
SAPD Radio Off Tick: 0, FIPS Change Tick: 0, LMS change Tick: 0, LMS IP:
172.16.1.250,
Mesh Ctrl Socket: 10, Hostapd Recreate Pending: FALSE, Hostapd PID: 3256,
Hostapd Sent Config: TRUE, Hostapd Sync Count: 0,
Mesh Radios Status:
Radio 0, Phy Down: FALSE, Band: 1, Current Channel: 149/0,
Total 25 channels:
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,
153,157,161,165,
```

```

Scan Active: FALSE, Scan Started 21528 Ticks, Scanned 0 channels, Curring
Scanning Channel 36,
Schedule Renegotiate: 0, Renegotiate: 0, Authenticate Pending: 0, Assoc
Pending: 0, Assoc Tick: 21528, WPA Auth Pending 0,

Marginal Uplink: FALSE, Hop Count: 0, Past Cost CH: 0, Path Cost: 0,
Children Num: 0, Node Cost: 0, Subtree Weight: 0,
Commit Pending: 0, Mesh_P VAP Up: TRUE, Point Radar Tick: 0, Radar Channel:
0,
Radio 1, Phy Down: FALSE, Band: 0, Current Channel: 6/0,
Total 11 channels: 1,2,3,4,5,6,7,8,9,10,11,
Scan Active: FALSE, Scan Started 21529 Ticks, Scanned 0 channels, Curring
Scanning Channel 1,
Schedule Renegotiate: 0, Renegotiate: 0, Authenticate Pending: 0, Assoc
Pending: 0, Assoc Tick: 21529, WPA Auth Pending 0,
Marginal Uplink: FALSE, Hop Count: 0, Past Cost CH: 0, Path Cost: 0,
Children Num: 0, Node Cost: 0, Subtree Weight: 0,
Commit Pending: 0, Mesh_P VAP Up: TRUE, Point Radar Tick: 0, Radar Channel:
0,
Mesh Configurations:
Max children: 64, Max Hop Count: 8, Heartbeat Threshold: 10, Roaming:
FALSE/RSSI-limit 0, Prefer Uplink Radio: No prefer uplink radio, Remote Mesh
MPV: 0
Metric Algorithm: Distribute Tree RSSI, Reselection Mode: Anytime, Optimize
Scan Interval: 120(s), Link Threshold: 12, Max RSSI: 38, RSSI Delta: 1,
Penalty: 10, Offset: 0
HT Enabled: 1, VHT Enabled: 1, HE Enabled: 1, 40M: 1, 80M: 1, 160M: 1
Mesh Access List Type: Deny, Hostname list(0):

```

Command History

Release	Modification
ArubaOS 8.8.0.0	The output parameters, Optimize Scan Interval and Optimize Scan Tick were introduced.
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh monitor

```
show ap mesh monitor
  info [ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>]
  stats [ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>]
```

Description

This command shows the mesh monitor information of APs.

Parameter	Description
info	Shows topology info of a mesh node.
stats	Shows statistics of a mesh link.
ap-name <ap-name>	Shows AP mesh log messages for the specified AP name.
bssid <bssid>	Shows AP mesh log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP mesh log messages for the specified IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap mesh neighbors

```
show ap mesh neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
[names]
```

Description

This command shows all mesh neighbors for an AP.

Parameter	Description
ap-name <ap-name>	Show mesh neighbors for an AP with a specific name.
bssid <bssid>	Show mesh neighbors for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show mesh neighbors for an AP with a specific IP address by entering its IP address in dotted-decimal format.
names	If you include this optional parameter, the Portal column in the output of this command will translate the BSSIDs of mesh parent and child APs to AP names (where available).

Example

In the example below, the output has been split into two tables to better fit on the page. In the actual CLI, the output appears in a single, wide table.

The **Flags** column in the output of this command indicates the high-throughput (HT) properties of the mesh node. In the example below, the string "HT-40MHzsgi-2ss" indicates that the node uses a 40MHz channel with a short guard interval (sgi) and sends 2 spatial streams (ss) (For versions prior to ArubaOS 8.9.0.0).

```
(host) [mynode] #show ap mesh neighbors ap-name portal

Neighbor list
-----
Radio      MAC          Portal          Channel  Age  Hops  Cost
Relation   Flags  RSSI  Rate Tx/Rx
---      ---  ---  -----
-----
0          00:0b:86:e8:09:d1  00:1a:1e:88:01:f0  157      0   1    11.00
C 3h:15m:42s  -      65    54/54
0          00:1a:1e:88:02:91  00:1a:1e:88:01:f0  157      0   1     4.00
C 3h:35m:30s  HL      59    300/300
0          00:0b:86:9b:27:78  Yes                157      0   0    12.00
N 3h:22m:46s  VLmK    26    -
0          00:0b:86:e8:09:d0  00:1a:1e:88:01:f0  157      0   1    11.00
N 3h:15m:36s  -      65    -
```

```

0          00:1a:1e:88:02:90 00:1a:1e:88:01:f0 157+    0    1    2.00
N 3h:35m:6s HL      59      -

```

A-Req	A-Resp	A-Fail	HT-Details	Cluster ID
1	1	0	Unsupported	sw-ad-GB32
1	1	0	HT-40MHzsgi-2ss	sw-ad-GB322
0	0	0	Unsupported	mc1
0	0	0	Unsupported	sw-ad-GB32
0	0	0	HT-40MHzsgi-2ss	sw-ad-GB32

```

Total count: 5, Children: 2
Relation: P = Parent; C = Child; N = Neighbor; B = Blacklisted-neighbor/Denylisted-neighbor
Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure; H = High Throughput; L = Legacy allowed
K = Connected, U = Upgrading, G = Descendant-upgrading; Z = Config pending; Y = Assoc-resp/Auth pending
a = SAE Accepted; b = SAE Blacklisted-neighbour/Denylisted-neighbour; e = SAE Enabled; u = portal-unreachable; o = opensystem; m = Mobility Enabled

```

The following example displays the mesh neighbor details for AP-635 access point in ArubaOS 8.9.0.0 or later versions.

```

show ap mesh neighbors ap-name ap635-4

Neighbor list
-----
Radio MAC              AP Name  Portal  Channel  Band  Age  Hops  Cost
Relation              Flags  RSSI  Rate Tx/Rx  A-Req  A-Resp  A-Fail  HT-
Details              Cluster ID
-----  ---
-----  -----
2      cc:88:c7:41:3d:30  ap635-3  Yes      169S    6GHz  0    0    1.00  P
22h:20m:10s          ELK    48    2401/0    2      2      0      HE-
160MHzsgi-2ss  jiajunname

Total count: 1, Children: 0
Relation: P = Parent; C = Child; N = Neighbor; B = Denylisted-neighbor
Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure; H = High Throughput; V = Very High Throughput, E= High efficient, L = Legacy allowed
K = Connected; U = Upgrading; G = Descendant-upgrading; Z = Config pending; Y = Assoc-resp/Auth pending
a = SAE Accepted; b = SAE Denylisted-neighbour; e = SAE Enabled; u = portal-unreachable; o = opensystem; m = Mobility Enabled

```

The output of this command includes the following information:

Column	Description
Radio	Identifies which radio the mesh neighbor belongs to.
MAC	MAC address of the mesh node.
AP Name (ArubaOS 8.9.0.0 or later versions)	Name of the mesh AP.
Portal	By default, this column displays the BSSID of the mesh point. If you include the optional <code>names</code> parameter, this column will display AP names, if available. The AP names will include [p] (parent), or [c] (child) suffixes to indicate the role of the mesh BSSID.
Channel	Number of a radio channel used by the AP.
Band (ArubaOS 8.9.0.0 or later versions)	The radio band for the mesh AP.
Age	Number of seconds elapsed since the AP heard from the neighbor.
Hops	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node
Cost	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Relation	Shows the relationship between the specified AP and the AP on the neighbor list and the amount of time that relationship has existed. <ul style="list-style-type: none"> ▪ P = Parent ▪ C = Child ▪ N = Neighbor ▪ B = Blacklisted-neighbor/Denylisted-neighbor
Flags	This parameter shows additional information about the mesh neighbor. The key describing each flag appears at the bottom of the neighbor list.

Column	Description
RSSI	The RSSI value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Rate Tx/Rx	The rate, in Mbps, that a neighbor transmits data to or receives data from the mesh-node specified by the command.
A-Req	Number of association requests from clients
A-Resp	Number of association responses from the mesh node
A-Fail	Number of association failures
Cluster	Name of the Mesh cluster that includes the specified AP or BSSID.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were made: <ul style="list-style-type: none"> All instances of <code>Blacklisted-neighbour</code> have been replaced with <code>Denylisted-neighbour</code>. The output of the command was modified to display the <code>AP Name</code> and <code>Band</code> parameters.
ArubaOS 8.8.0.0	The output of the command was modified to display the <code>m</code> flag.
ArubaOS 8.7.0.0	The output was modified to include the <code>Radio</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh tech-support

```
show ap mesh tech-support ap-name <ap-name> <filename>
```

Description

This command shows all information for an AP, and saves that information in a file on the controller. This command displays the output of the multiple mesh and debug CLI commands, then saves that data into a report file on the controller's flash drive, where it can be analyzed for debugging purposes. The information in this report includes the output of the following commands:

- [show ap mesh neighbors](#)
- [show ap mesh debug current-cluster](#)
- [show ap mesh debug provisioned-clusters](#)
- [show ap mesh debug counters](#)
- [show ap mesh debug forwarding-table](#)
- [show ap mesh debug meshd-log](#)
- [show ap mesh debug hostapd-log](#)

Parameter	Description
<ap-name>	Name of an AP for which you want to create a report.
<filename>	Filename for the report created by this command. The file can only be saved in the flash directory. If desired, you can use FTP or TFTP to copy the file to another destination.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh topology

```
show ap mesh topology [long] [page <page>] [start <start>]
```

Description

This command shows the mesh topology tree.

Parameter	Description
long	Include the names of a mesh portal's children in the output of this command.
page <page>	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
start <start>	Start displaying the mesh topology tree at a chosen index number by entering the index number of the AP at which command output should start.

Examples

An **(N)** in the **Mesh Role** column indicates the node is 11N capable. An **(N)** beside the parent name in the **Parent** column indicates that the mesh node's the parent is also 11N capable.

```
(Aruba9012_DA_90_B0) [mynode] # show ap mesh topology

Mesh Cluster Name: jiajunname
-----
Name      State  IP Address      Switch IP      Mesh Role      Radio  BSSID
  Parent  Path Cost  Node Cost  Link Cost  Hop Count  RSSI  Rate
Tx/Rx    Last Update  Uplink Age  #Children
-----
-
-----
ap635-3  ACTV   10.10.117.253  10.65.255.117  Portal (HE)    2
cc:88:c7:41:3d:30 -      0          1          0          0          -
-          52s        22h:37m:11s 1
ap635-4  ACTV   10.10.117.252  10.65.255.117  Point (HE)     2
cc:88:c7:41:2c:e0 ap635-3 1          0          0          1          48
2401/0    3m:6s     22h:20m:30s 0

Total APs :2
(R): Recovery AP. (N): 11N Enabled. (AC): 11AC Enabled. (AD): 11AD Enabled.
(HE): 11AX Enabled. For Portals 'Uplink Age' equals uptime.
ACTV: Active on controller, REPL: Replicated on controller.
```

The output of this command includes the following information:

Column	Description
Name	Name of the mesh node.
State	State of the mesh node.
IP Address	IP address of the mesh node.
Switch IP	IP address of the controller.
Mesh Role	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
Radio	Mesh radio number of the AP.
BSSID	BSSID for the AP. This is usually the AP's MAC address.
Parent	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal.
Path Cost	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Node Cost	A relative measure of the quality of the node, where a lower number of is more favorable than a higher number. This cost is related to the number of children on the specified node.
Link Cost	A relative measure of the quality of the link. For example, a more congested link will have a higher link cost than a similar, less-congested link.
Hop Count	Number of hops to the mesh portal.
RSSI	The RSSI value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Rate Tx/Rx	The rate, in Mbps, that a mesh point transmits and receives at on its uplink. Note that the rate information is only as current as indicated in the Last Update column.
Last Update	Time elapsed since the mesh node last updated its statistics.
Uplink Age	Time elapsed since the mesh node became active in the mesh topology.
#Children	Number of children associated with a parent mesh point.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output was modified to include the <code>Radio</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh-cluster-profile

```
show ap mesh-cluster-profile [<profile>]
```

Description

This command shows configuration settings for a mesh cluster profile. The command **show ap mesh-cluster-profile** displays a list of all mesh cluster profiles configured on the Mobility Conductor, including the number of references to each profile and each profile's status. Include the optional <profile> parameter to show detailed settings for an individual mesh cluster profile.

Parameter	Description
<profile>	Name of a mesh cluster profile

Examples

The example below shows the configuration settings for the mesh cluster profile "meshcluster2".

```
(host)[mynode] #show ap mesh-cluster-profile meshcluster2

Mesh Cluster profile "meshcluster2"
-----
Parameter      Value
-----
Cluster Name   company-mesh
RF Band        a
Encryption     opensystem
WPA Hexkey     N/A
WPA Passphrase N/A
```

The output of this command includes the following information:

Parameter	Description
Cluster Name	Name of the mesh cluster using this profile
RF band	The RF band in which the AP should operate: <ul style="list-style-type: none">■ g = 2.4 GHz■ a = 5 GHz
Encryption	Data encryption setting for the mesh cluster profile. <ul style="list-style-type: none">■ opensystem—No authentication and encryption.■ wpa2-psk-aes—WPA2 with AES encryption using a preshared key.

Parameter	Description
WPA Hexkey	The WPA PSK (only for mesh cluster profiles using WPA2 with AES encryption).
WPA Passphrase	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Related Commands

Command	Description
ap mesh-cluster-profile	This command configures a mesh cluster profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on managed devices.

show ap mesh-ht-ssid-profile

show ap mesh-ht-ssid-profile [<profile>]

Description

This command shows configuration settings for a mesh high-throughput Service Set Identifier (SSID) profile. High-throughput APs support additional settings not available in legacy APs. A mesh high-throughput SSID profile can enable or disable high-throughput (802.11n) features and 40 Mhz channel usage, and define values for aggregated MAC protocol data units (MDPUs) and Modulation and Coding Scheme (MCS) ranges.

This command shows a list of all mesh high-throughput SSID profiles configured on the Mobility Conductor, including the number of references to each profile and each profile's status. Include the optional <profile> parameter to show detailed settings for an individual mesh high-throughput SSID profile.

Parameter	Description
<profile>	Name of a mesh high-throughput SSID profile.

Examples

The example below shows the configuration settings for the mesh high-throughput radio profile "default".

```
(host) [mynode] #show ap mesh-ht-ssid-profile default

Mesh High-throughput SSID profile "default"
-----
Parameter                                     Value
-----
40 MHz channel usage                           Enabled
BA AMSDU Enable                                Enabled
Temporal Diversity Enable                       Disabled
High throughput enable (SSID)                  Enabled
Legacy stations                                 Allowed
Low-density Parity Check                       Enabled
Maximum number of spatial streams usable for STBC reception 1
Maximum number of spatial streams usable for STBC transmission 1
MPDU Aggregation                               Enabled
Max received A-MPDU size                        65535 bytes
Max transmitted A-MPDU size                     65535 bytes
Min MPDU start spacing                          8 usec
Short guard interval in 20 MHz mode             Enabled
Short guard interval in 40 MHz mode             Enabled
Supported MCS set                               0-23
Explicit Transmit Beamforming                   Disabled
```

Transmit Beamforming Compressed Steering	Enabled
Transmit Beamforming non Compressed Steering	Enabled
Transmit Beamforming delayed feedback support	Enabled
Transmit Beamforming immediate feedback support	Enabled
Transmit Beamforming Sounding Interval	1800 sec

The output of this command includes the following information:

Column	Description
40 MHz channel usage	This parameter shows if the profile enables or disables the use of 40 MHz channels.
BA AMSDU Enable	Shows if the AP has enabled or disabled the ability to receive AMSDU in BA negotiation.
Temporal Diversity Enable	Shows if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries.
High throughput enable (SSID)	Shows if 802.11n high-throughput features are enabled or disabled for this profile. By default, high-throughput features are enabled.
Legacy stations	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
Low-density Parity Check	If enabled, the AP will advertise LDPC support. LDPC improves data transmission over radio channels with high levels of background noise.
Maximum number of spatial streams usable for STBC reception	Shows the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.) NOTE: If transmit beamforming is

Column	Description
	enabled, STBC will be disabled for beamformed frames.
Maximum number of spatial streams usable for STBC transmission	Shows the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on 170 Series, 130 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.) NOTE: If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
MPDU Aggregation	Shows if the profile enables or disables MPDU aggregation.
Max received A-MPDU size	Configured maximum size of a received aggregate MPDU, in bytes.
Max transmitted A-MPDU size	Configured maximum size of a transmitted aggregate MPDU, in bytes.
Min MPDU start spacing	Configured minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
Supported MCS set	Displays a list of MCS values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node.
Short guard interval in 20 MHz mode	Shows if the profile enables or disables use of short (400ns) guard interval in 20 MHz mode.
Short guard interval in 40 MHz mode	Shows if the profile enables or disables use of short (400ns) guard interval in 40 MHz mode.
Explicit Transmit Beamforming	Shows if Explicit Transmit Beamforming is enabled or disabled for 130 Series APs.

Column	Description
	NOTE: If this parameter is disabled, the other transmit beamforming configuration settings have no effect.
Transmit Beamforming Compressed Steering	When enabled, the AP can use explicit compressed feedback from clients to obtain a steering matrix. (For 130 Series APs only.)
Transmit Beamforming non Compressed Steering	When enabled, the AP can use explicit noncompressed feedback from clients to obtain a steering matrix. (For 130 Series only)
Transmit Beamforming delayed feedback support	Shows if the AP has enabled or disabled delayed feedback/report support in Transmit Beamforming. (For 130 Series only)
Transmit Beamforming immediate feedback support	Shows if the AP has enabled or disabled immediate feedback/report support in Transmit Beamforming. (For 130 Series only)
Transmit Beamforming Sounding Interval	Time interval in seconds between updates of Transmit Beamforming channel estimation. (For 130 Series only)

Related Commands

Command	Description
ap mesh-ht-ssid-profile	This command configures a mesh HT SSID profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh-radio-profile

show ap mesh-radio-profile [<profile>]

Description

This command shows configuration settings for a mesh radio profile. The radio profile determines the radio frequency/channel used only by mesh nodes to establish mesh links. Mesh nodes operating in different cluster profiles can share the same radio profile. Conversely, mesh portals using the same cluster profile can be assigned different mesh radio profiles to achieve frequency separation.

This command shows a list of all mesh radio profiles configured on the controller, including the number of references to each profile and each profile's status. Include the optional <profile> parameter to show detailed settings for an individual mesh radio profile.

Parameter	Description
<profile>	Name of a mesh radio profile.

Example

The example below shows the configuration settings for the mesh cluster profile "default".

```
(host) [mynode] #show ap mesh-radio-profile default
Mesh Radio profile "default"
-----
Parameter                                     Value
-----
802.11a Transmit Rates                        6 9 12 18 24
36 48 54
802.11g Transmit Rates                        1 2 5 6 9 11
12 18 24 36 48 54
Allowed VLANs on mesh link                    1-4094
BC/MC Rate Optimization                       Enabled
Heartbeat threshold                           10
Link Threshold                                12
Maximum Children                              64
Maximum Hop Count                             8
Mesh Private Vlan                             0
Mesh High-throughput SSID Profile             default
Mesh Survivability                           Disabled
Metric algorithm                              distributed-
tree-rssi
Rate Optimization for delivering EAPOL frames and mesh echoes Disabled
Reselection mode                              startup-
subthreshold
Retry Limit                                   8
RTS Threshold                                 2333 bytes
```


Mesh Mobility	Disabled
Mobility RSSI Threshold	15
Mobility Beacon Miss Number	16

The output of this command includes the following information:

Parameter	Description
802.11a Transmit Rates	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
802.11g Transmit Rates	Indicates the transmit rates for the 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
Allowed VLANs on mesh link	Specify a list of VLAN IDs that can be used by a mesh link on APs associated with this mesh radio profile
BC/MC Rate Optimization	If enabled, the mesh node will use the slowest associated mesh-point rate for broadcast/multicast data (rather than minimum).
Heartbeat Threshold	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes before the mesh node is considered inactive and is dropped as a mesh neighbor.
Link Threshold	Indicates the threshold for the lowest acceptable RSSI value. Links that drop below this threshold will have an increased link cost. Default: 12.

Parameter	Description
Maximum Children	The maximum number of children a mesh portal can accept.
Maximum Hop Count	The maximum number of hops allowed between a mesh point and a mesh portal.
Mesh Private Vlan	This parameter is experimental and reserved for future use.
Mesh High-throughput SSID Profile	The High-throughput SSID Profile associated with this mesh radio profile.
Mesh Survivability	This parameter shows if mesh points and portals can become active even if the controller cannot be reached by bridging LAN traffic. This is a beta feature that is disabled by default; it should not be enabled unless you are instructed to do so by Aruba technical support.
Metric algorithm	Algorithm used by a mesh node to select its parent.
Rate Optimization for delivering EAPOL frames and mesh echoes	If this option is enabled, mesh APs will use a more conservative rate for more reliable delivery of EAPOL frames.
Reselection Mode	<p>Specifies one of the following methods used to find a better mesh link.</p> <ul style="list-style-type: none"> startup-sub-threshold: When bringing up the mesh network, mesh nodes have 3 minutes to find a better uplink. After that time, each mesh node evaluates alternative links only if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). The reselection process is canceled if the average RSSI rises on the existing uplink rises above the configured link threshold.

Parameter	Description
	<ul style="list-style-type: none"> ■ reselect-any-time: Connected mesh nodes evaluate alternative mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal. ■ reselect-never: Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal. ■ subthreshold-only: Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.
Retry Limit	Maximum number of times a mesh node can re-send a packet.
RTS Threshold	The packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue RTS and wait for other mesh nodes to respond with CTS to begin transmission. This helps prevent mid-air collisions.
Mesh Mobility	Displays if fast roaming on a mobility mesh point is enabled or disabled based on low RSSI or missed beacon frames.
Mobility RSSI Threshold	Displays the RSSI threshold value of the parent to indicate fast roaming on a mobility mesh point.
Mobility Beacon Miss Number	Displays the number of consecutive missed beacon frames to indicate fast roaming on a mobility mesh point.

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.8.0.0	The output of the command was modified to display the following parameters: <ul style="list-style-type: none"> ■ Mesh Mobility ■ Mobility RSSI Threshold ■ Mobility Beacon Miss Number
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap mesh-recovery-profile

show ap mesh-recovery-profile

Description

This command shows the mesh recovery-profile information.

Example

The following example shows the mesh recovery-profile information:

```
(host) [mynode] #show ap mesh-recovery-profile

AP Mesh Recovery Profile
-----
Item                Value
----                -
Cluster Name       RecoveryRVOCDoNgqKqDEGOZ
RF Band            a
WPA Hexkey         *****
WPA Passphrase     N/A
Encryption         wpa2-psk-aes
```

Related Commands

Command	Description
ap mesh-radio-profile	This command configures a mesh radio profile used by mesh nodes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap modem-download-log

show ap modem-download-log

Description

This command displays the logs when the Remote AP downloads the Aruba USB LTE modem firmware from the managed device.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example displays the logs for download of Aruba USB LTE modem firmware on a Remote AP.

```
(host) [mynode] #show ap modem-download-log
downloading now
Download file ArubaOS_90xx_lte_fw_v20_77807
fetching ('tftp -g -r ArubaOS_90xx_lte_fw_v20_77807 -l ArubaOS_90xx_lte_fw_
v20_77807 144.37.254.3 ')
Success: Download image successful.
cleanup exit
done
```

Command History

Version	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

show ap modem-upgrade-status

show ap modem-upgrade-status [page <page> | start <start>]

Description

This command displays the status of Aruba USB LTE modem upgrade on Remote APs.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
page <page>	Displays the number of entries in each page of the command output.
start <start>	Displays the command output at the specified index value.

Example

The following example displays the status of Aruba USB LTE modem firmware upgrade on Remote APs.

```
(host) [mynode] #show ap modem-upgrade-status
AP modem upgrade status
-----
Item                               Value
----                               -
Status                             Inactive
Mode                               All APs
Image Source                        None
Max Simultaneous Downloading       10
current Simultaneous Downloading   0
Start Time
Current Status                     Not Start

AP Status Summary
-----
AP State  Count
-----  -----
Updating 1
TOTAL 1

AP Modem Upgrade Status
-----
AP Name          AP Group AP Mac          AP Serial #  AP IP          AP
Type
-----          -
-----
20:4c:03:a4:a6:85 ap-20x   20:4c:03:a4:a6:85  CNJSKSM011   192.168.229.2
505H

Upgrade State  Start Time          End Time  Failure Count  Failure Reason
-----
Updating      2021-07-28  08:02:24  0
```

Related Command

Command	Description
ap modem-upgrade	This command configures the firmware upgrade of Aruba USB LTE modem.

Command History

Version	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

show ap monitor

```
show ap monitor
  active-laser-beams
  ap-list
  arp-cache
  association
  channel
  client-list
  containment-info
  debug
  ids-state
  mesh-list
  pot-ap-list
  pot-client-list
  routers
  scan-info
  stats
    advanced {[[ap-name <ap-name>]][ip-addr <ip-addr>]][ip6-addr <ip6-addr>]
      [client-mac <client-mac>]][bssid <bssid>]}
  wired-mac
```

Description

This command shows information for Aruba Air Monitors.

Parameter	Description
active-laser-beams	Show active laser beam generators. The output of this command shows a list of all APs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which AP is sending out deauthorization frames, although it does not specify which AP is being contained.
ap-list	Show list of APs being monitored.
arp-cache	Show ARP cache of learned IP to MAC binding.
association	Show association table for an AP.
channel	Show state and stats of a specific channel.
client-list	Show list of client being monitored.
containment-info	Show containment events and counters triggered by the wired containment and wireless containment features configured in the ids general-profile . The output of this command shows device and target data for wired containment activity.

Parameter	Description
debug	Show the Air Monitor debugging information.
ids-state	Show IDS state.
mesh-list	Show list of mesh APs being monitored.
pot-ap-list	Display the potential AP table.
pot-client-list	Display the potential client table.
routers	Show Router MAC Addresses learned. The output of this command includes the router's MAC address, IP address and uptime.
scan-info	Show AP scanning information.
stats	Shows statistics for an AP or a client.
wired-mac	Show Wired MAC Addresses learned.

Command History

Release	Modification
ArubaOS 8.7.0.0	<p>The output of the following commands was modified to include IPv6 field:</p> <ul style="list-style-type: none"> ▪ <code>show ap monitor arp-cache ap-name <ap_name></code> ▪ <code>show ap monitor debug status ap-name <ap_name></code> ▪ <code>show ap monitor containment-info ap-name <ap_name></code>
ArubaOS 8.6.0.0	<p>A new interface for Radio 2 was displayed for the following parameters:</p> <ul style="list-style-type: none"> ▪ <code>show ap monitor containment-info</code> ▪ <code>show ap monitor debug</code> ▪ <code>show ap monitor scan-info</code> <p>The output displayed the following bss color related information:</p> <ul style="list-style-type: none"> ▪ bss-color ▪ partial bss color ▪ bss color disabled
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor active-laser-beams

```
show ap monitor active-laser-beams {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows the active laser beam generators.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.
band <band>	Shows the radio band. Possible values are 2.4GHz, 5GHz, or 6GHz. NOTE: The 6GHz value is applicable to Wi-Fi 6E APs only.
channel <channel>	Shows the AP channel.

Example

The following example lists the active laser beam sources for a specific BSSID:

```
(host)[mynode] (config) #show ap monitor active-laser-beams bssid
f4:2e:7f:0b:a8:80
Active Laser Beam Sources
-----
bssid  channel  rssi  ap name  lms ip  master/ conductor ip  inactive time
-----
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The 6GHz value was added to <code>band <band></code> parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor ap-list

```
show ap monitor ap-list
  ap-name <ap-name> {containment-exclusion} | {wifi-direct [ all ]} | {verbose}
  bssid <bssid>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

This command shows the list of APs being monitored.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
containment-exclusion	Shows details of vendor specific IE information for containment exclusion.
verbose	Shows additional information about flags and the flag, W is displayed to identify the Wi-Fi direct devices. This flag will be displayed only if the detection of WIFI-Direct P2P groups is enabled in the IDS unauthorized device profile.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example displays the Monitored AP table, which lists all the APs monitored by a specified AP or BSSID (For versions prior to ArubaOS 8.9.0.0).

```
(host) #show ap monitor ap-list ap-name all2

Monitored AP Table
-----
bssid          essid          chan  ap-type          phy-type
  dos          dt/mt          ut/it          -----
-----
  ---          -----          -----
24:de:c6:be:c3:fa  bridge-85      161  interfering      80211a-
HT-40  disable  33633/17957  0/0
24:de:c6:8e:aa:86  ap214-tb2-%aprf%  11  interfering
```

```

80211b/g-HT-20  disable  33633/33633  0/0
24:de:c6:be:b7:3a  bridge-85          64    interfering          80211a-
HT-40    disable  33633/17065  8/4

encr          nstas  avg-snr  curr-snr  avg-rssi  curr-rssi  wmacs  ibss
cl-delay  bss-color  partial bss color  bss color  disabled
-----
-----
wpa2-psk-aes  0      37      37      57      58      0      no
0            3      false
open         0      53      55      41      40      0      no
0            3      false
wpa2-psk-aes  0      45      45      49      50      0      no
0            59     false

```

The following example displays the Monitored AP table, which lists all the APs monitored by a specified AP or BSSID (ArubaOS 8.9.0.0 or later versions).

```

(host) #show ap monitor ap-list ap-name hhm-635

Monitored AP Table
-----
bssid          essid          band/chan/ch-width/ht-type
6GHz capable  ap-type      dos      dt/mt          ut/it      encr
nstas  avg-snr  curr-snr  avg-rssi  curr-rssi  wmacs  ibss  cl-delay
bss-color  partial bss color  bss color  disabled
-----
-----
-----
cc:88:c7:41:64:60  8@hzm-635-psk          6GHz/37S/160MHz/HE
yes                valid          disable  781198/781198  0/0          wpa3-sae-aes
0                 25            25       70           70           0           no           0           14
false
1c:28:af:68:1f:f0  6GHz_DUT          6GHz/49E/80MHz/HE
yes                interfering    disable  781185/124537  3/0          wpa3-sae-aes
0                 24            25       70           70           0           no           0           35
false
1c:28:af:67:ef:60  zz-635-wpa3-owe          6GHz/1E/80MHz/HE
yes                interfering    disable  374985/1926    103/0        wpa3-owe-aes
0                 0             8         0            87           0           no           0           56
false
1c:28:af:68:66:40  11                6GHz/37+/40MHz/HE
yes                interfering    disable  270423/157932  0/0          wpa3-sae-aes
0                 30            32       64           63           0           no           0           29
false
1c:28:af:68:40:33  000-owe-6g          6GHz/37+/40MHz/HE
yes                interfering    disable  161381/161381  0/0          wpa3-owe-aes
0                 25            26       69           69           0           no           0           23
false
1c:28:af:68:66:41(*)  060606          6GHz/37+/40MHz/HE
yes                interfering    disable  124188/124188  124188/0     wpa3-sae-aes
0                 0             0         0            0            0           no           0           29
false

```

```

1c:28:af:68:40:34(*) 000-non-cnsa-6g 6GHz/37+/40MHz/HE
yes interfering disable 92522/92522 92522/0 wpa3-other-
gcm256 0 0 0 0 0 no 0
23 false false
1c:28:af:68:40:36(*) 000-cnsa-6g 6GHz/37+/40MHz/HE
yes interfering disable 92521/92521 92521/0 wpa3-other-
gcm256 0 0 26 0 69 0 no 0
23 false false
1c:28:af:68:28:c0 jiyong-remote 6GHz/37+/40MHz/HE
yes interfering disable 27207/27207 0/0 wpa3-sae-aes
0 8 9 86 86 0 no 0 56
false false
1c:28:af:68:55:c0 ethersphere-arubaos-6g 6GHz/197E/80MHz/HE
yes interfering disable 26999/8500 13/4 wpa3-sae-aes
0 6 7 89 88 0 no 0 2
false false
cc:88:c7:41:25:30 6GHz/85/20MHz/non-HT
yes interfering disable 962/134 962/134 unknown
0 0 0 0 0 no 0 ---
--- ---
Start:0
Length:11
Total:11
Current max monitor size:2048
(*): Non-transmitted BSSID

```

The output of this command includes the following parameters:

Parameter	Description
bssid	BSSID of an AP. This is usually the AP's MAC address.
ssid	ESSID that names a wireless network.
chan (For versions prior to ArubaOS 8.9.0.0)	Radio channel used by the BSSID.
band/chan/ch-width/ht-type (ArubaOS 8.9.0.0 or later versions)	The AP radio type displayed as radio band/channel number/channel bandwidth/throughput type.
6Ghz capable (ArubaOS 8.9.0.0 or later versions)	Shows whether the AP supports 6 GHz radio band.

Parameter	Description
ap-type	Shows classification of the AP.
phy-type (For versions prior to ArubaOS 8.9.0.0)	Radio PHY type. Possible types include: <ul style="list-style-type: none"> ■802.11a ■802.11a-HT-40 ■802.11b/g ■802.11b/g-HT-20
dos	Shows if the feature to contain DoS attacks has been enabled or disabled.
dt/mt	dt: Detected time: the number of timer ticks since the AP was last detected. mt: Monitor time; the number of elapsed timer ticks since the AP first recognized the monitored AP.
ut/it	ut: Unseen time: the number elapsed timer ticks the monitored AP was not seen when scanning a channel of the device. it: AP idle time, the number of timer ticks since the AP last saw any frames from the monitored AP.
encr	Shows the encryption type of the BSSID. If there are multiple encryption types, this command shows the lowest encryption type.
nstas	Shows the number of stations connected to the AP (as seen by the monitoring AP).

Parameter	Description
avg-snr	Shows the average SNR.
curr-snr	Shows the current SNR.
avg-rssi	Shows the average RSSI for the device. NOTE: RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.
curr-rssi	Shows the current RSSI for the device.
wmacs	Shows the number of unique wireless MAC addresses seen on the Wi-Fi network from the AP's BSSID.
ibss	Shows all the monitored APs (BSSIDs).
cl-delay	Shows the delay in classification of each device. NOTE: The maximum delay for clients is not displayed if the <code>unclass_sta_update</code> parameter is not enabled.
bss-color	Shows the bss color selected. Range: 1-63
partial bss color	Shows if it is partial bss enabled.
bss color disabled	Shows if the bss color configuration is disabled.

The following example displays all the WIFI-Direct devices detected by a specified AP.

```
(host) #show ap monitor ap-list ap-name 635-ac wifi-direct all

WIFI Direct Devices
-----
BSSID          SSID          GO   assoc cli  Dev Caps
Grp Caps  Rap Type      DOS  Hosted
-----
-----
18:60:24:36:8f:e1  DIRECT-E0-HP OfficeJet 4650  yes  0          0x05
0x01             interfering no    no
28:3b:82:cc:49:f6  Hevnoraak's Mind  yes  1          0x25
0xAB             interfering no    no
```

The following example displays the details of vendor specific IE information for containment exclusion.

```
(host) #(mynode) #show ap monitor ap-list ap-name 655-ee containment-
exclusion
AP Containment Exemption
-----
bssid          ssid          ap-type      exemption-rule-index
exemption-rule-criteria
-----
-----
34:8a:12:f7:b6:c0  S28_AP655    interfering  1
8C:FD:F0  4
cc:88:c7:41:83:40  S06_Test     interfering  1
8C:FD:F0  4
cc:88:c7:41:75:a0  S20_6ghz     valid       1
8C:FD:F0  4
cc:88:c7:41:83:41  S06-US-5Ghz-24Ghz  interfering  1
8C:FD:F0  4
00:5f:67:5a:d3:8a  Deco_Competitive_Lab  interfering  1
8C:FD:F0  4
06:5f:67:5a:d3:8a             interfering  1
8C:FD:F0  4
06:5f:67:5a:d3:8b             interfering  1
8C:FD:F0  4
00:5f:67:5a:d3:8b  Deco_Competitive_Lab  interfering  1
8C:FD:F0  4
cc:88:c7:41:95:80  S06-US-6Ghz-only  interfering  1
8C:FD:F0  4
cc:88:c7:41:83:20  S06-US-6Ghz-only  interfering  1
8C:FD:F0  4
34:8a:12:f8:15:20  S06-US-6Ghz-only  interfering  1
8C:FD:F0  4
cc:88:c7:41:95:a0  S06_Test     interfering  1
8C:FD:F0  4
cc:88:c7:41:95:a1  S06-US-5Ghz-24Ghz  interfering  1
8C:FD:F0  4
00:5f:67:72:15:0c  tp-link_Omada  interfering  1
8C:FD:F0  4
```

```

34:8a:12:f7:b6:d0 S28_AP655          interfering 1
8C:FD:F0 4
d0:4d:c6:b6:93:e0          valid      1
8C:FD:F0 4

```

Related Command

Command	Description
show ap monitor debug	This command shows information for an Air Monitor's current status, message counters, or profile settings.

Command History

Release	Modification
ArubaOS 8.11.1.0	A new sub-parameter, verbose was added to the show ap monitor ap-list ap-name <ap-name> command.
ArubaOS 8.11.0.0	The <code>containment-exclusion</code> and <code>wifi-direct[all]</code> sub-parameters were introduced.
ArubaOS 8.9.0.0	The command output was modified to include the following: <ul style="list-style-type: none"> Removed <code>chan</code> and <code>phy-type</code> parameters. Added <code>band/chan/ch-width/ht-type</code> and <code>6Ghz capable</code> parameters.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor arp-cache

```
show ap monitor arp-cache {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}
```

Description

This command shows the ARP/NDP cache of learned IP to MAC bindings.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Examples

The following example shows the ARP/NDP cache table of learned IPv4 address:

```
(host) [mynode] (config) #show ap monitor arp-cache ip-addr 10.65.47.250  
  
br0:10.65.47.250  
ARP/NDP Cache Table  
-----  
mac                ip                ipv6                vlanid  age  
---                --                ----                -      -  
e8:f7:24:46:49:b9  10.65.47.193     fe80::eaf7:24ff:fe46:49b9  0  
9h:3m:13s  
70:3a:0e:cc:ee:1e  10.65.47.251     -                        0  
9h:3m:13s  
94:b4:0f:c8:85:96  0.0.0.0          fe80::96b4:fff:fec8:8596  0  
9h:3m:13s  
tun1:10.65.47.250
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor association

```
show ap monitor association {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows the association table for an Air Monitor (AM).

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example lists the MAC addresses associated with the Air Monitor BSSID (For versions prior to ArubaOS 8.9.0.0).

```
(host) #show ap monitor association ap-name ap9 00:1a:1e:11:74:a1
Association Table
-----
mac                rsta-type  auth  phy-type
---                -
00:1d:d9:01:c4:50  valid      yes   80211a
00:17:f2:4d:01:e2  valid      yes   80211a
00:1f:3b:8c:28:89  valid      yes   80211a
00:1d:d9:05:05:d0  valid      yes   80211a
00:14:a4:25:72:6d  valid      yes   80211a
00:19:7d:d6:74:8d  valid      yes   80211a
```

The output of this command includes the following parameters:

Column	Description
mac	MAC address associated with the Air Monitor BSSID

Column	Description
<pre>rsta-type</pre>	Rogue station type: <ul style="list-style-type: none"> ■ interfering: Interfering station. ■ valid: Station is not a rogue station. ■ DoS: Station may have attempted a DoS attack.
<pre>auth</pre>	Displays a yes if the client has been authenticated.
<pre>phy-type</pre> (For versions prior to ArubaOS 8.9.0.0)	The RF band in which the AP should operate: <ul style="list-style-type: none"> ■ 802.11g = 2.4 GHz ■ 802.11a = 5 GHz
<pre>band</pre> (For ArubaOS 8.9.0.0 or later versions)	The RF band in which the AP should operate. Displays one of the following values: <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz(For Wi-Fi 6E APs)

Related Command

Command	Description
am	The <code>scan</code> sub-command enables channel scanning for the specified air monitor. In addition, the <code>test</code> sub-command enables the client to test an air monitor.

Command History

Release	Modification
ArubaOS 8.9.0.0	<p>The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions):</p> <ul style="list-style-type: none"> ■ Replaced <code>phy-type</code> with <code>band</code> ■ Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for <code>band</code> output parameter respectively. ■ Introduced 6GHz value for <code>band</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

0		100/0/0							
52	0	0	0	0	36	0	0	98	
1		88/1/12							

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor client-list

```
show ap monitor client-list {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows the list of clients being monitored.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Examples

The following example shows the table of monitored clients (For versions prior to ArubaOS 8.9.0.0).

```
(host) [mynode] (config) #show ap monitor client-list ip-addr 10.65.47.250

Monitored Client Table
-----
mac          bssid          essid          channel
sta-type    auth phy-type    dt/mt          ut/it          snr  rssi  cl-delay
---          -
-----
c8:b5:ad:ba:fd:80 a8:bd:27:fa:cb:95 test-open      52E
interfering no 80211a-VHT-80 769/37         223/10         49  46   -
48:45:20:03:dc:2a f0:5c:19:1e:e9:b1 9@535-hhm-psk 64E
interfering yes 80211a-VHT-80 23234/921     293/15         40  55   -
24:f2:7f:3a:77:00 a8:bd:27:fa:cb:94 hide-test      52E
interfering no 80211a-VHT-80 6632/216     19/48         44  51   -
18:64:72:7e:54:71 a8:bd:27:fa:cb:93 test-psk-wifi 52E
interfering yes 80211a-VHT-80 19661/3272   142/6          39  56   -
70:3a:0e:87:8a:90 d8:c7:c8:b1:0a:f1 gran-uplink-stability 157+
interfering yes 80211a-HT-40 1518/1518    2/1           45  50   -
```

The following example shows the table of monitored clients for a Wi-Fi 6E AP (For ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #show ap monitor client-list ap-name hhm-635

Monitored Client Table
-----
mac          bssid          band/chan/ch-width/ht-type  6GHz
capable  essid          sta-type        auth dt/mt          ut/it          snr  rssi  cl-
delay
---          -
d8:f8:83:35:f7:64  1c:28:af:68:11:20  6GHz/37S/160MHz/HE          yes
    liying-635  interfering  yes  2370/2370  339/338  14  81  -
Start:0
Length:1
Total:1
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> Replaced <code>phy-type</code> with <code>band/chan/ch-width/ht-type</code> parameter. Introduced <code>6GHz capable</code> parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor containment-info

```
show ap monitor containment-info {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows the AP containment activity.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The output of the command lists the wired containment counters for a BSSID:

```
(host) *[mynode] (config) #show ap monitor containment-info bssid ac:a3:1e:57:82:40
```

```
wifi0: Wireless Containment Counters
```

```
-----  
Parameter                                     Value  
-----  
Last Deauth Timer Tick                        0  
Deauth frames to AP                          0  
Deauth frames to Client                      0  
Last Tarpit Timer Tick                       0  
Tarpit Frames: Probe Response                0  
Tarpit Frames: Association Response          0  
Tarpit Frames: Authentication                0  
Tarpit Frames: Data from AP                  0  
Tarpit Frames: Data from Client              0  
Last Enhanced Adhoc Containment Timer Tick  0  
Enhanced Adhoc Containment: Frames To Data Sender 0  
Enhanced Adhoc Containment: Frames To Data Receiver 0  
Enhanced Adhoc Containment: Response to Request 0  
Enhanced Adhoc Containment: Replay Response  0
```

```
wifi1: Wireless Containment Counters
```

```
-----
```

```

Parameter                                     Value
-----
Last Deauth Timer Tick                       0
Deauth frames to AP                          0
Deauth frames to Client                      0
Last Tarpit Timer Tick                       0
Tarpit Frames: Probe Response                0
Tarpit Frames: Association Response           0
Tarpit Frames: Authentication                0
Tarpit Frames: Data from AP                  0
Tarpit Frames: Data from Client              0
Last Enhanced Adhoc Containment Timer Tick    0
Enhanced Adhoc Containment: Frames To Data Sender 0
Enhanced Adhoc Containment: Frames To Data Receiver 0
Enhanced Adhoc Containment: Response to Request 0
Enhanced Adhoc Containment: Replay Response    0

br0: Wired Containment Counters
-----
Parameter                                     Value
-----
Last Wired Containment Timer Tick             0
Last Tagged Wired Containment Timer Tick      0
Spoof frames sent                            0
Spoof frames sent on tagged vlan              0

tun1: Wired Containment Counters
-----
Parameter                                     Value
-----
Last Wired Containment Timer Tick             0
Last Tagged Wired Containment Timer Tick      0
Spoof frames sent                            0
Spoof frames sent on tagged vlan              0

Wired Containment Activity
-----
Device-Type  Device-MAC  Target-MAC  Target-IPv4  Target-IPv6
-----

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor debug

```
show ap monitor debug
  counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
  profile-config {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
  status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
    am-scan|ap-radio|apsystem|
    arm|event-thresholds|ids-dos|ids-general|ids-impersonation|ids-
    signaturematching|
    ids-unauthorized-device|interference|regulatory-domain|rf-behavior
```

Description

This command shows information for an Air Monitor's current status, message counters, or profile settings.

Parameter	Description
counters	Shows the maximum classification delay that was observed in monitored APs and clients, the number of Unclassified Device messages that were sent to the WMS, and the number of monitored APs/clients that were present in those messages. This parameter also shows the number of monitored APs/clients that were created and removed by the AP. This information is captured on an hourly basis for the last 24 hours. NOTE: The maximum delay for clients is not displayed if the unclass_sta_update parameter is not enabled.
profile-config	Shows the configuration received by the AP for each profile.
status	Shows general AP status information and the maximum classification delay that was observed in monitored APs and clients, in the WLAN Interface option. NOTE: The maximum delay for clients is not displayed if the unclass_sta_update parameter is not enabled.
ap-name <ap-name>	Show data for an AM with a specific name.
bssid <bssid>	Show data for an AM with a specific BSSID. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AM with a specific IP address by entering its IPv4 address in dotted-decimal format.

Parameter	Description
ip6-addr <ip6-addr>	Show data for an AM with a specific IP address by entering its IPv6 address in dotted-decimal format.
am-scan	Show Air Monitor active scanning configuration.
ap-radio	Show the Air Monitor radio configuration parameters, as defined in the AM's 802.11a, 802.11b, or high-throughput radio profiles.
ap-system	Show an Air Monitor's system configuration settings, as defined in its AP System profile.
arm	Show an Air Monitor's ARM settings, as defined in its current ARM profile
event-thresholds	Show an Air Monitor Event Thresholds settings, as defined in its current RF Event Thresholds profile
ids-dos	Show an Air Monitor IDS DoS settings, as defined in its current IDS DoS profile.
ids-general	Show an Air Monitor IDS General Configuration settings, as defined in its IDS General profile.
ids-impersonation	Show an Air Monitor IDS Impersonation Configuration settings, as defined in its IDS Impersonation profile.
ids-signature-matching	Show an Air Monitor IDS Signature Matching configuration settings, as defined in its IDS Signature Matching profile
ids-unauthorized-device	Show an Air Monitor IDS Unauthorized Device configuration settings, as defined in its IDS Unauthorized Device profile.
interference	Show an Air Monitor's interference configuration settings, as defined in its current RF Optimization profile.
regulatory-domain	Show an Air Monitor's Regulatory Domain configuration settings, as defined in its Regulatory Domain profile.
rf-behavior	Show an Air Monitor RF Behavior Configuration

Examples

The output of the following command includes the *WLAN Interface*, *Data Structures*, *WLAN InterfaceSwitch Status* and *RTLS Configuration* tables for the specified AP.

```
(host) #show ap monitor debug status ap-name ap12
WLAN Interface
-----
```

```

bssid          scan   monitor  probe-type      phy-type        task
channel  pkts
-----
--  ----
00:1a:1e:11:5f:10  enable  enable  sap             80211a-HT-40    tuned  153
496970814
00:1a:1e:11:5f:00  enable  enable  airmatch-am     80211b/g-HT-20  tuned  6
391278179

Wired Interface
-----
mac          ip          gw-ip        gw-mac        status
pkts
---
----

macs gw-macs tagged-pkts vlan
-----
00:1a:1e:c9:15:f0  192.0.2.32.200      192.0.2.32.254  00:0b:86:08:e1:00
enable 101960
2 3 1 03
Global Counters
-----
key          value
---
-----
Packets Read      888248993
Bytes Read        2819670134
Num Interrupts    681037971
Num Buffer Overflows 591393
Max PPS           16239
Cur PPS          1130
Max PPI           20
Cur PPI          2
Uptime           3323085
AP Name          AL12
LMS IP
Master/Conductor IP
AP Type          125
Country Code     2

```

Starting from ArubaOS 8.4.0.0, the output of the command `show ap monitor debug status` includes the new counters to differentiate the distribution of DATA, MGMT, CTRL, and AGGR packets.

```

WLAN packet counters for DATA
-----
Interface          Data Pkts Data Bytes Data Max PPS Data Cur PPS Data
Max BPS Data Cur BPS
-----
-----
18:64:72:7e:51:d0(wifi0) 67730      3045300    366          5
36600          140
18:64:72:7e:51:c0(wifi1) 0          0          0          0          0
0

```

WLAN packet counters for MGMT

```

-----
Interface                MGMT Pkts  MGMT Bytes  MGMT Max PPS  MGMT Cur PPS
MGMT Max BPS  MGMT Cur BPS
-----
18:64:72:7e:51:d0(wifi0) 2835404    750667644    217           31
60416           8512
18:64:72:7e:51:c0(wifi1) 0          0            0            0
0              0
    
```

WLAN packet counters for CTRL

```

-----
Interface                CTRL Pkts  CTRL Bytes  CTRL Max PPS  CTRL Cur PPS
CTRL Max BPS  CTRL Cur BPS
-----
18:64:72:7e:51:d0(wifi0) 5466191    106264680    6910          28
132428         512
18:64:72:7e:51:c0(wifi1) 0          0            0            0
0              0
    
```

WLAN packet counters for AGGR

```

-----
Interface                FIRST AGGR  MIDDLE AGGR  LAST AGGR  TOTAL AGGR  NUM
NON AGGR
-----
84:d4:7e:d1:d7:d0(wifi0) 4059       3452         4147       11658
95687
84:d4:7e:d1:d7:c0(wifi1) 0          0            0          0          0
    
```

Data Structures

```

-----
ap  sta  pap  psta  ch  msg-hash  ap-1
--  ---  ---  ---  --  -
20  40   17   55   24  21       20
    
```

Other Parameters

```

-----
key                value
---
WMS on Master/Conductor    disabled
Stats Update Interval    60
Poll Interval            174000
Num Switches             1
Collect Stats            enabled
    
```

WLAN Interface Switch Status

```

-----
Bssid                Type  Status  Last-reg  N-reg  Last-update  Next-update
N-updates  Last-ack
-----
-----
    
```

```

00:1a:1e:11:5f:10 local up      3321891  3821  3322965  197
10368          3322965
00:1a:1e:11:5f:00 local up      3321891  3821  3322917  187
10378          3322965

```

RTLS Configuration and State

```

-----
Type          Server IP  Port  Freq  Active  Rpt-Tags  Tag-Mcast-Addr
-----
MMS           N/A       N/A   N/A   *       disable   01:0c:cc:00:00:00
Aer scout     2001::3   N/A   30    *       disable   00:00:00:00:00:00
RTLS          2001::2   N/A   20    *       disable   01:18:8e:00:00:00

```

```

-----
Tags-Sent     Rpt-Sta  Incl-Unassoc-Sta  Sta-Sent  Cmpd-Msgs-Sent
-----
N/A           disable  N/A                N/A       N/A
N/A           enable   disable            2610     265
N/A           enable   enable

```

The output of this command includes the following parameters:

Column	Description
bssid	BSSID for the AP. This is usually the AP's MAC address.
scan	Indicates whether or not if active scanning is enabled on this AP.
monitor	Indicates whether the AP radio is currently enabled or disabled.
probe-type	This parameter displays one of the following options to show the AP is configured. <ul style="list-style-type: none"> ■ sap: Default AP setting. ■ am: AP is configured as an Air Monitor. ■ m-portal: AP is configured as a Mesh portal. ■ m-point: AP is configured as a Mesh point. ■ airmatch-am: AP is configured in AP monitoring mode.
task	This parameter displays one of the following options to show the radio's current task: <ul style="list-style-type: none"> ■ scan: AP is scanning other channels. ■ tuned: AP is tuned on one channel. ■ locate: AP has been asked to locate a specific AP or client. ■ pcap: The AP is enabled with the Packet Capture feature.
channel	The radio channel currently used by an AP's WLAN interface.
pkts	Number of packets seen on the interface.

Column	Description
mac	MAC address for the AP's wired interface.
ip	The AP's IP address.
gw-ip	IP address for the AP's gateway.
gw-mac	MAC address for the AP's gateway.
status	Shows if the interface is currently enabled or disabled.
pkts	Number of packets seen on the AP's wired interface.
macs	Number of MAC addresses in the Wired MAC table for that interface.
gw-macs	Number of MAC addresses in the Wired MAC table for that interface.
tagged-pkts	Number VLAN-tagged packets sent to that interface.
vlan	The VLAN ID for the packets sent to that interface.
Packets read	Number of packets read by the AP since it was last reset.
Bytes read	Number of bytes read by the AP since it was last reset.
Num Intercepts	Number of interrupts from the AP's driver.
Num Buffer Overflows	Number of times excessive traffic has filled the AP's buffers.
Max PPS	Maximum throughput rate seen on the interface, in packets per second.
Cur PPS	Current throughput rate seen on the interface, in packets per second.
Max PPI	Maximum interrupt rate seen on the interface, in interrupts per second.
Cur PPI	Current interrupt rate seen on the interface, in interrupts per second.
Uptime	Number of seconds since the AP was last reset.
LMS IP	IP address of the AP's managed device
Master/Conductor IP	IP address of the AP's Mobility Conductor.
AP type	AP model type.

Column	Description
Country Code	The AP's country code. Valid radio channels for your wireless network are based on your country code. If you change the AP's country code, the valid channels will be reset to the defaults for the new country.
ap	Number of other APs monitored by this AP.
sta	Number of clients and APs seen by this AP.
pap	Number of potential APs; APs which have transmitted a beacon, but have not yet been registered.
psta	Number of potential stations; AP has seen a MAC address from the station but hasn't yet received traffic from it.
ch	Number of channel entries in the channel table.
msg-hash	Number of different message types seen on the interface.
ap-1	(For internal use only)
WMS on Master/Conductor	Indicates if the AP communicates to the wms process on Mobility Conductor or a managed device. enabled: Communicates with Mobility Conductor. disabled: Communicates with a managed device only.
Stats Update Interval	If the AP is collecting statistics, this value is the interval in seconds in which the AP sends statistics to the WMS process.
Poll Interval	Interval, in milliseconds, that the AP sends RSSI updates to the WMS process.
Num Switches	Number of controllers to which this AP has access. If the value is 1, the AP has access to Mobility Conductor <i>or</i> a managed device. If the value is 2, the AP has access to Mobility Conductor <i>and</i> a managed device.
Collect Stats	If enabled, the AP will collect statistics to send to the WMS process.
Bssid	BSSID of the radio.
Type	Indicates whether the controller type is master (Mobility Conductor) or local (managed device).
Status	If up , the AP can reach the managed device. If down , the AP cannot reach the managed device.
Last-reg	The time the AP last registered with the WMS process.
N-reg	Number of times the AP has registered with the WMS process.

Column	Description
Last-update	The last timer tick time the AP updated the WMS process.
Next-update	Interval between the last update and the next scheduled update.
N-updates	Number of updates sent to the WMS process.
Last-ack	Number of timer ticks since the AP received an acknowledgment from the WMS process.
Type	Type of RTLS server used by the AP, such as MMS or Aeroscout.
Server IP	IP address of the RTLS server.
Port	Port used by the RTLS server.
Frequency	Rate, in seconds, at which RTLS messages are sent to the server.
Active	Indicates if the server is active on the AP.
Rpt-Tags	Displays whether tag reporting is enabled or not.
Tag-Mcast-Addr	Displays MAC OUI of the tags that are forwarded to the server.
Tags-Sent	Displays the cumulative count of the tag reports sent to server.
Rpt-Sta	Displays whether station reporting is enabled or not.
Incl-Unassoc-Sta	Displays whether unassociated stations are included in station reporting or not.
Sta-Sent	Displays cumulative count of station reports sent to server.
Cmpd-Msgs-Sent	Displays cumulative count of compound messages containing station reports sent to server.

Starting from ArubaOS 8.11.0.0, the output of the `show ap monitor debug status` command includes new counters that list discarded and detected Apple Wireless Direct Link (AWDL) frames.

```

AM AWDL Counters (wifi0)
-----
Parameter                Value
-----
Dropped AWDL frames      0
Detected AWDL frames     1171

```

The output of this command includes the following parameters:

Column	Description
Parameter	Type of Apple Wireless Direct Link frame.
Value	Number of Apple Wireless Direct Link frames that are dropped or detected.

Related Command

Command	Description
show ap monitor	This command shows information for Aruba Air Monitors.

Command History

Release	Modification
ArubaOS 8.11.0.0	The following modifications were introduced: <ul style="list-style-type: none"> ■ The output of the <code>show ap monitor debug status</code> command includes new counters that list detected and discarded Apple Wireless Direct Link frames. ■ The output of the show ap monitor debug profile-config command includes the details of containment exclusion.
ArubaOS 8.10.0.0	The probe type airmatch-am was introduced in the output of the command under WLAN Interface table.
ArubaOS 8.9.0.0	The output was modified to include the following changes: <ul style="list-style-type: none"> ■ Replaced <code>phy-type</code> with <code>band/chan/ch-width/ht-type</code>. ■ Replaced <code>802.11g</code> and <code>802.11a</code> with <code>2.4GHz</code> and <code>5GHz</code>. ■ Introduced <code>6GHz</code> parameter for Wi-Fi 6E APs. All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.8.0.0	The output was modified to include zero wait DFS channel details.
ArubaOS 8.4.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The <code>ip6-addr</code> parameter was added. ■ The output of the <code>show ap monitor debug status</code> command displays both IPv4 and IPv6 addresses. ■ The output of the <code>show ap monitor debug status</code> command includes new counters to differentiate the

Release	Modification
	distribution of DATA, MGMT, CTRL, and AGGR packets.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor ids-state

```
show ap monitor ids-state {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}  
    block-ack|dsta|events|general|mac-oui|mitm|omerta|ps-  
    dos|rate|sequence|signature|spoofed-frames|valid-ssid|wpa-ft
```

Description

This command shows the IDS state for AP monitor.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
block-ack	Show current sequence number windows for block ACKs.
dsta	Show deauth station monitoring state.
events	Show most recent IDS events.
general	Show general IDS configuration.
mac-oui	Show MAC OUI tables.
mitm	Show statistics that are being monitored to detect channel based Man in the Middle.
omerta	Show statistics that are being monitored to detect Omerta attack.
ps-dos	Show statistics that are being monitored to detect Power Save DoS attack.
rate	Show rate check state.
sequence	Show sequence analysis state.
signature	Show signature state.
spoofed-frames	Show count of frames that were spoofed to look as if they were from VAPs on this AP.
valid-ssid	Show valid and protected SSIDs.
wpa-ft	Show WPA FT Attack Detection state.

Example

The following example shows the deauth station monitoring state table:

```
(host) [mynode] (config) #show ap monitor ids-state bssid ac:a3:1e:57:82:52
dsta

Disconnect Station State Table
-----
MAC                Quiet time  Index  Rx Assoc Resp Pkt Count  Tx/Rx
Deauth/Disassoc Pkt Count
---
-----
ac:a3:1e:57:82:52  0          9      0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0
Interval: 10 seconds
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor mesh-list

```
show ap monitor mesh-list {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}
```

Description

This command shows the list of mesh APs being monitored.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example lists the mesh AP table:

```
(host) [mynode] (config) #show ap monitor mesh-list bssid ac:a3:1e:57:82:52  
  
Monitored Mesh Table  
-----  
bssid          essid          chan  ap-type  
  phy-type      dos      dt/mt      ut/it  encr      nstas  avg-snr  
curr-snr  avg-rssi  curr-rssi  wmacs  ibss  cl-delay  bss-color  partial  bss  
color  bss color  disabled  mesh-portal-id  
-----  
-----  
-----  
9c:1c:12:fe:4e:91  1          64E  interfering  
  80211a-VHT-80  disable  35890/2332  5/0  wpa2-psk-aes  1  54  
55      40      40      0      no      0      ---      ---  
  ---          9c:1c:12:fe:4e:91  
38:17:c3:00:02:90  9f9036113b45d87abf1d84d383c0f13  36E  interfering  
  80211a-VHT-80  disable  35621/6183  44/1  wpa2-psk-aes  1  29  
28      65      67      0      no      0      ---      ---  
  ---          38:17:c3:00:02:90  
38:17:c3:92:03:31  031d02a9ea5861cadd40ef2979e89d7  44+  interfering  
  80211a-VHT-40  disable  35602/3875  10/0  wpa2-psk-aes  1  19  
40      76      55      0      no      0      ---      ---  
  ---          38:17:c3:92:03:31
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none">■ Replaced <code>phy-type</code> with <code>band/chan/ch-width/ht-type</code> parameter.■ Introduced <code>6GHz_capable</code> parameter for Wi-Fi 6E APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor pot-ap-list

```
show ap monitor pot-ap-list {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows potential AP list being monitored.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example shows the potential AP table:

```
(host) [mynode] (config) #show ap monitor pot-ap-list bssid
ac:a3:1e:57:82:52

Potential AP Table
-----
bssid          channel  phy      num-beacons  tot-beacons  num-frames  mt
  it   at  ibss      snr  rssi
-----  ---  -
--   --  ----
9c:8c:d8:7f:bd:d1  11      80211b  0            9            0            1
 16   1   disable  25   70
70:3a:0e:4e:eb:20  7        80211b  0            9            0            1
 19   1   disable  5    90
48:4a:e9:7c:91:01  6        80211b  0            9            0            25
 11   2   disable  25   70
9c:1c:12:89:31:42  1        80211b  0            9            0            3
 54   2   disable  8    87
38:17:c3:53:3f:20  11       80211b  0            9            0            7
 35   3   disable  31   64
```

The output of this command includes the following information:

Column	Description
bssid	The Basic Service Set Identifier of the AP.
channel (For versions prior to ArubaOS 8.9.0.0)	The current radio channel of the AP.
phy (For versions prior to ArubaOS 8.9.0.0)	The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b/g, 802.11b/g-HT-20.
band/chan (For ArubaOS 8.9.0.0 or later versions)	The current radio channel and RF band type.
num-beacons	Number of beacons seen during a 10-second scan.
tot-beacons	Total number of beacons seen since the last reset.
num-frames	Total number of frames seen since the last rest.
mt	Monitor time; the number of timer ticks elapsed since the controller first recognized the AP.
it	Idle time - expressed as a number of timer ticks.

Column	Description
at	Active time, in timer ticks.
ibss	Shows if adhoc BSS is enabled or disabled. It will be enabled if the BSSID has detected an adhoc BSS (an ibss bit in an 802.11 frame).
snr	Signal-to-Noise ratio.
rssi	The Receive Signal Strength Indicator (RSSI) value that represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> ■ Replaced <code>channel</code> and <code>phy</code> with <code>band/chan</code> parameter. ■ Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for <code>band/chan</code> output parameter respectively. ■ Introduced 6GHz value for <code>band/chan</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor pot-client-list

```
show ap monitor pot-client-list {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows potential client list being monitored.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example shows the potential client table (For versions prior to ArubaOS 8.9.0.0):

```
(host) [mynode] (config) #show ap monitor pot-client-list bssid
1d:b3:1e:57:17:20

Potential Client Table
-----
mac          last-bssid          from-bssid          to-bssid
mt      it  channel  snr  rssi  snr/rssi-age
---      --  -----  ---  ----  -----
--      --  -----  ---  ----  -----
d0:d3:e0:4f:9a:b0  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
231    11  157      52  43    12
48:51:b7:b8:2e:cd  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
3397   36  157      36  59    37
24:77:03:e7:a2:64  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
8756   36  132      48  47    37
4c:1d:96:e0:58:2b  d0:d3:e0:b2:dd:90  00:00:00:00:00:00  00:00:00:00:00:00
127    120 124      0   0     n/a
```

The following example shows the potential client table for a Wi-Fi 6E AP (For ArubaOS 8.9.0.0 or later versions):

```
(host) [mynode] (config) #show ap monitor pot-client-list ap-name hhm-635

Potential Client Table
-----
mac                last-bssid          from-bssid          to-bssid
mt  it  band/chan  snr  rssi  snr/rssi-age
---  --  -----  ---  ----  -----
--  --  -----  ---  ----  -----
fc:b3:bc:44:28:11  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  16  79  123144
fc:b3:bc:45:14:0b  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  15  80  1826
fc:b3:bc:44:19:25  1c:28:af:68:17:b2  1c:28:af:68:17:b2  00:00:00:00:00:00
0  0  6GHz/37  0  0  n/a
fc:b3:bc:45:28:38  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  4  91  649658
fc:b3:bc:45:27:de  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  14  81  617
fc:b3:bc:f2:5c:e2  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/53  6  89  17567
cc:88:c7:41:57:40  04:08:66:6d:01:08  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  4  91  1723044
14:18:c3:48:00:80  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  30  65  2360
d8:f8:83:35:f7:64  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  16  79  1175
cc:88:c7:41:3b:b1  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  18  77  83150
fc:b3:bc:44:27:f8  cc:88:c7:41:25:30  00:00:00:00:00:00  cc:88:c7:41:25:30
0  0  6GHz/85  5  90  787845
fc:b3:bc:44:1b:be  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  28  67  1206780
1c:28:af:68:39:10  ff:ff:ff:ff:ff:ff  00:00:00:00:00:00  00:00:00:00:00:00
0  0  6GHz/37  5  90  1192351
Num Potential Clients:13
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> Replaced channel with band/chan parameter. Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for band output parameter respectively. Introduced 6GHz value for band/chan parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor routers

```
show ap monitor routers {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}
```

Description

This command shows the router MAC addresses learned.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example lists the wired MAC addresses or potential wireless devices:

```
(host) [mynode] (config) #show ap monitor routers bssid cd:a9:1e:57:28:98  
  
Wired MAC of Potential Wireless Devices  
-----  
mac                ip                ipv6  age  
---                --                ----  ---  
00:0b:86:6c:75:dc  -                -     5s  
70:3a:0e:cc:ee:1e  10.65.47.251    -     5s  
00:0b:86:6c:75:dc  10.65.47.251    -     5s  
70:3a:0e:cc:ee:1e  10.65.47.251    -     5s
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor scan-info

```
show ap monitor scan-info {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}
```

Description

This command shows the AP scanning information.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example lists the AP scanning information:

```
(host) [mynode] (config) #show ap monitor scan-info bssid ac:a3:1e:57:82:52  
  
WIF Scanning State: wifi0: ac:a3:1e:57:82:50  
-----  
Parameter                               Value  
-----  
Probe Type                               sap  
Phy Type                                  80211a-VHT-80  
Scan Mode                                  all-reg-domain  
Scan Channel                              no  
Disable Scanning                          yes  
RegDomain Scan Completed                   yes  
DOS Channel Count                          0  
Current Channel                            157E  
Current Scan Channel                       132E  
Current Channel Index                      132  
Current Scan Start Milli Tick              37033110  
Current Dwell Time                         110  
Current Scan Type                           all-reg-domain  
  
Scan-Type-Info  
-----  
Info-Type           Active  Reg-domain  All-reg-domain  Rare  DOS
```



```

-----
Dwell Times          500    250    200    100    500
Last Scan Channel   36E    44E    132E   104+   0

WIF Scanning State: wifi1: ac:a3:1e:57:82:40
-----
Parameter            Value
-----
Probe Type           sap
Phy Type             80211b/g-HT-20
Scan Mode            all-reg-domain
Scan Channel         no
Disable Scanning    yes
RegDomain Scan Completed yes
DOS Channel Count    0
Current Channel      6
Current Scan Channel 8+
Current Channel Index 8
Current Scan Start Milli Tick 37033450
Current Dwell Time   110
Current Scan Type    all-reg-domain

Scan-Type-Info
-----
Info-Type           Active  Reg-domain  All-reg-domain  Rare  DOS
-----
Dwell Times        500    250    200    100    500
Last Scan Channel  12-    8+    13-    0    0

```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following changes (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for <code>Phy Type</code> output parameter respectively. Introduced 6GHz value for <code>Phy Type</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor stats

```
show ap monitor stats {advanced}|{ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows packet, signal, and channel statistics for an AP or a client.

Parameter	Description
advanced	Show advanced statistics for an AP or client.
ap-name <ap-name>	Show statistics for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show data for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example shows monitoring statistics for the AP ap305, and a client with the MAC address d8:6c:02:99:bc:7a:

```
(host) #show ap monitor stats ap-name ap305 mac d8:6c:02:99:bc:7a verbose

Aggregate Stats
-----
retry   low-speed   non-unicast   recv-error   frag   bwidth
-----
0       0           0             0            0     0
RSSI
----
avg-signal  low-signal  high-signal  count  duration (sec)
-----
51          51          51           4      50
Monitored Time:6626
Last Packet Time:585500
Uptime:585502

AMPDU Tx Stats
-----
```

```

tx-non-ampdu-pkt  tx-ampdu-pkt  tx-filtered-pkt  tx-ampdu-byte
-----
0                0              0                0
tx-filtered-bytes tx-first-pkt  tx-middle-pkt   tx-last-pkt
-----
0                0              0                0
AMPDU Rx Stats
-----
tx-non-ampdu-pkt  tx-ampdu-pkt  tx-filtered-pkt  tx-ampdu-byte
-----
0                7              66               73102
tx-filtered-bytes tx-first-pkt  tx-middle-pkt   tx-last-pkt
-----
66639            0              0                7

DoS Frames
-----
tx  old-tx  rx  old-rx
--  -----  --  -----
0  0        0  0
Interference Baseline
-----
FRR  FRER
---  ----
17  4
Handoff Assist
-----
rssi-index  cur-signal  old-cur-signal
-----
0           51          0
High Throughput Parameters
-----
ht-type  primary-channel  sec-channel  gf-supported  40mhz-intolerance
-----
none     0                0            0             0

```

The output of this command includes the following parameters:

Column	Description
retry	Percent of 802.11 retry frames sent because a client failed to send an ACK.
Low-speed	Percent of frames sent at a data rate of 18 Mbps or slower.
non-unicast	Percent of non-unicast frames
recev-error	Percent of error frames of all frames seen in the last second.
frag	Rate of fragmented packets, in frames per second

Column	Description
bwth	Current bandwidth, in bps.
avg-signal	Average signal-to-noise ratio over the interval since the AP's last reset.
low-signal	Lowest signal-to-noise ratio over the interval since the AP's last reset.
high-signal	Highest signal-to-noise ratio over the interval since the AP's last reset.
count	Number of packets seen on the AP over the interval since the AP's last reset.
Duration	Time over which the AP has measured RSSI values.
tx	The total number of deauthorization frames sent to this MAC address for containment in the interval from the AP's last reset until the current timer tick.
old-tx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
rx	The total number of deauthorization frames spoofing the MAC address in the interval from the AP's last reset until the current timer tick.
old-rx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
FRR	Frame retry rate, in frames per second.
FRER	Frame error retry rate, in frames per second.
rss-index	This value indicates the number of consecutive timer ticks over which the value of the RSSI of the client has reduced by more than 3 units. NOTE: This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile.
cur-signal	The RSSI of the most recent frame received from the specified MAC address.
old-cur-signal	The most recent RSSI of the MAC which is 3 lower or 5 higher than the current RSSI. NOTE: This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile
ht-type	This parameter indicates support for the following HT types:

Column	Description
	no : No support for high-throughput. HT-20 : Support for 20 Mhz high-throughput only. HT-40 : Support for 40 Mhz high-throughput.
primary-channel	Primary radio channel.
sec-channel	Secondary radio channel
gf-supported	If 1 , this AP supports greenfield mode. If 0 , greenfield is not supported.
40mhz-intolerance	Indicates whether the specified MAC address is 40 Mhz intolerant.

Related Commands

Command	Description
show ap monitor debug	This command shows information for an Air Monitor's current status, message counters, or profile settings.
show ap monitor	This command shows information for Aruba Air Monitors.

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the <code>show ap monitor stats</code> command was modified to display the additional debug counter information.
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap monitor wired-mac

```
show ap monitor wired-mac {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|  
{ip6-addr <ip6-addr>}  
ap-bssid|config|enet-mac|gw-mac|oui-prop|system-gw-mac|system-wired-mac
```

Description

This command shows the wired MAC addresses learned.

Parameter	Description
ap-name <ap-name>	Shows data for an AM with a specific name.
bssid <bssid>	Shows data for an AM with a specific BSSID. The BSSID is usually the AM's MAC address.
ip-addr <ip-addr>	Shows data for an AM with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AM with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.
ap-bssid	Specify BSSID of monitored AP.
config	Display Configured Wired MACs.
enet-mac	Display wired MACs learned at AM ENET Interface.
gw-mac	Display Gateway MACs learned at AM ENET Interface.
oui-prop	Display OUI propagation information.
system-gw-mac	Display gateway MACs learned at the controller.
system-wired-mac	Display wired MACs learned at the controller.

Example

The following example shows the wired MAC address table:

```
(host) [mynode] (config) #show ap monitor wired-mac bssid ac:a3:1e:57:82:52  
ap-bssid ac:a3:1e:57:82:52
```

```
Wired MAC Table
```

```
-----
```

```
mac   age
```

```
---   ---
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap multizone-profile

```
show ap multizone-profile <profile-name>
```

Description

This command shows details of an AP MultiZone profile.

Parameter	Description
<profile-name>	The name of an existing AP MultiZone profile.

Example

The following example displays the MultiZone profile and also provides the number of datazones and number of virtual APs available in the primary zone:

```
(host) (config) ##show ap multizone-profile MZoneProfile

Multizone Enabled

Multizone Table
-----
Zone  IP Address   IPv6 Address      Max Vaps Allowed  Max Nodes Allowed
Description
----  -
0     N/A          N/A               2                 1
N/A
2     10.15.144.5  2001:1001::201   3                 1

Number of datazones:1
```

Related Command

Command	Description
ap multizone-profile	MultiZone feature allows AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain. The zone can have a single managed device or a cluster. This command allows you to create an AP MultiZone profile, set the data zone index, and controller-ip.

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the <code>show ap multizone-profile</code> command was modified to display the IPv6 Address and Description columns.
ArubaOS 8.0.1.0	The <code>num-nodes</code> sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on managed devices.

show ap owe-tm-info

```
show ap owe-tm-info
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  wired-mac <wired-mac>
```

Description

This command shows information about OWE Transition VAPs generated.

Parameter	Description
ap-name <ap-name>	Shows OWE Transition VAPs generated on the AP with this name.
ip-addr <ip-addr>	Shows OWE Transition VAPs generated on the AP with IPv4 address.
ip6-addr <ip6-addr>	Shows OWE Transition VAPs generated on the AP with IPv6 address.
wired-mac <wired-mac>	Shows OWE Transition VAPs generated on the AP with MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show ap packet-capture

```
show ap packet-capture status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

This command shows the status of outstanding packet capture (pcap) sessions. The Packet Capture (pcap) feature copies control path packets from the Aruba Control Processor, providing visibility for packets to or from the controller. This provides a useful troubleshooting tool for diagnosing communication problems with elements such as a Radius server. You can retrieve these packets by issuing the command `tar logs`, and then viewing the file `filter.pcap` on the controller's flash drive.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Example

The following example shows the Packet Capture Sessions table for an AP named **AP16**:

```
(host) #show ap packet-capture status ap-name AP16
Packet Capture Sessions
-----
pcap-id  filter  type  intf          channel max-pkt-size  num-pkts
status   url    target
-----  -
1         raw    00:1a:1e:82:ab:b0  161
```

The output of this command includes the following parameters:

Column	Description
pcap-id	ID number of the packet capture session.
filter	Packet Capture filter specification.

Column	Description
type	A raw packet capture type indicates that the controller is streaming raw packets to an external viewer.
intf	BSSID of the interface for the PCAP session.
channel	Channel used by AP to capture packets.
max-pkt-size	Maximum size of all captured packets.
num-pkts	Number of packets captured during the session.
status	Shows the current status of the packet-capture session.
url	Packet capture data can be downloaded to this URL.
target	IP address of the client station running Wildpacket's AiroPeek monitoring application.

Related Command

Command	Description
packet-capture	Use this command to enable or disable packet capturing and set packet capturing options for a single packet capture session.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap papi-err

```
show ap papi-err {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows the PAPI error messages.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show data for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following example displays the status of PAPI send error messages:

```
(host) #show ap papi-err
STM SAP PAPI Send Error
-----
Name  bssid  ip   Tunnel Add  Tunnel Remove  Arp Req  Vlan Req  Sta Req
Mcast Req
-----
-----
```

Related Command

Command	Description
papi-security	This command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap port status

```
show ap port status {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|wired-mac <wired-mac>}
```

Description

This command shows the status of the AP's wired ports. The status is updated every 60 seconds.

Parameter	Description
ap-name <ap-name>	Name of the AP.
bssid <bssid>	BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
wired-mac <wired-mac>	MAC address of the AP.

Example

The following example shows the wired port status of an AP named **LocalAP1**. In this example, the output is divided into multiple sections to fit better on the pages of this document. In the actual CLI, it appears in a single long table.

```
(host) #show ap port status ap-name LocalAP1

AP "LocalAP1" Port Status (updated every 60 seconds)
-----
Port  MAC              Type  Forward Mode  Admin   Oper   Speed
Duplex 802.3az PoE
----  ---
-  -----  ---
0    00:1a:1e:10:05:1a  GE    N/A          enabled  up    1 Gb/s  full
  N/A      N/A
1    00:1a:1e:10:05:1b  FE    tunnel       enabled  up    100 Mb/s full
  N/A      N/A
2    00:1a:1e:10:05:1c  FE    tunnel       enabled  down  N/A     N/A
  N/A      N/A
3    00:1a:1e:10:05:1d  FE    N/A          disabled down  N/A     N/A
  N/A      N/A

STP          TX-Packets  TX-Bytes  RX-Packets  RX-Bytes
---          -
N/A          23697      3338307   27449       8471871
Forwarding   12185      6593226   18436       1758272
Disabled     0          0         0           0
```

Off 0 0 0 0

Related Command

Command	Description
ap wired-port-profile	This command configures a wired port profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap power-mgmt-statistics

```
show ap power-mgmt-statistics {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows the power status statistics of an AP connected to a managed device. Issue this command to get power status statistics of an AP connected to a managed device.

Parameter	Description
ap-name <ap-name>	Shows the statistics of the specified AP name.
ip-addr <ip-addr>	Shows the specified IP address.
ip6-addr <ip6-addr>	Shows the specified IPv6 address.

Example

The following example shows the power statistics of an AP connected to a managed device:

```
(host) #show ap power-mgmt-statistics ap-name 00:4e:35:c4:47:06
AP Power Mgmt Status, Last update at 2019-09-26 16:43:13
-----
Attr          Value
----          -
LLDP Granted Power Eth 0: 23.3 Eth 1: 23.3
LLDP Request Power Eth 0: 23.3 Eth 1: 23.3
Temperature      Highest temperature: 52°C, Lowest temperature: 48°C,
Current temperature: 50°C
Power Supply      POE-AT
USB Status        USB Knob: Auto, USB Status: Disabled
PSE Status        N.A.
ETH Status        Eth 0:Enabled. Eth 1:Disabled.
G-radio Chain     4*4
G-radio Enable    Enabled
G-radio Power     Full Power
A-radio Chain     4*4
A-radio Enable    Enabled
A-radio Power     Full Power
CPU Throttle      100%
Power Consumption 7.6W
IPM Enable        Disabled
ITM Status        Thermal Standby
```

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>ITM Status</code> parameter was added.
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
530 Series and 550 Series access points	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap profile-usage

```
show ap profile-usage {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

This command shows a complete list of all profiles referenced by an individual AP or an AP BSSID. Use this command to monitor the configuration profiles in use by an AP or a specific BSSID. The output of this command shows the name of each profile type that is associated with the AP or BSSID, as well as the source that associates the profile with the AP.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. The BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Example

The following example shows the list of all profiles associated with the AP or BSSID:

```
(host) [mynode] (config) #show ap profile-usage ap-name ac:a3:1e:cd:78:24
AP "ac:a3:1e:cd:78:24" Profiles
-----
Profile Type                Profile                Source
-----
AP system profile          deauth_all            ap-group
"deauth_all" ap-system-profile
Dump collection profile    deauth_all            ap
system-profile "deauth_all" dump-collection-profile
802.11 60GHz radio profile default                ap-group
"deauth_all" dot11-60GHz-radio-profile
Regulatory Domain profile test                    ap-group
"deauth_all" regulatory-domain-profile
RF Optimization Profile    default                ap-group
"deauth_all" rf-optimization-profile
RF Event Thresholds Profile default                ap-group
"deauth_all" event-thresholds-profile
IDS General Profile        default                ids
profile "default" general-profile
IDS Rate Thresholds Profile default                ids dos-
profile "default" assoc-rate-thresholds
IDS Rate Thresholds Profile default                ids dos-
profile "default" disassoc-rate-thresholds
```

```

IDS Rate Thresholds Profile      default          ids dos-
profile "default" deauth-rate-thresholds
IDS Rate Thresholds Profile      probe-request-response-thresholds  ids dos-
profile "default" probe-request-rate-thresholds
IDS Rate Thresholds Profile      probe-request-response-thresholds  ids dos-
profile "default" probe-response-rate-thresholds
IDS Rate Thresholds Profile      default          ids dos-
profile "default" auth-rate-thresholds
IDS Signature Matching Profile    default          ids
profile "default" signature-matching-profile
IDS Denial Of Service Profile     default          ids
profile "default" dos-profile
IDS Impersonation Profile         default          ids
profile "default" impersonation-profile
IDS Unauthorized Device Profile   default          ids
profile "default" unauthorized-device-profile
IDS Profile                       default          ap-group
"deauth_all" ids-profile
ARM RF domain                    default          ap-group
"deauth_all" arm-rf-domain-profile
AP multizone profile             default          ap-group
"deauth_all" ap-multizone-profile
AM Filter                       default          ap-group
"deauth_all" am-filter-profile
AP group                         deauth_all
AP "ac:a3:1e:cd:78:24" Radio 0 Profiles
-----
Profile Type                      Profile      Source
-----
802.11a radio profile             default     ap-group "deauth_all"
dot11a-radio-profile
Adaptive Radio Management (ARM) profile default-a   rf dot11a-radio-profile
"default" arm-profile
High-throughput radio profile     default-a   rf dot11a-radio-profile
"default" ht-radio-profile
Spectrum profile                 default-a   rf dot11a-radio-profile
"default" spectrum-profile
AM Scanning profile              default     rf dot11a-radio-profile
"default" am-scan-profile
AP "ac:a3:1e:cd:78:24" BSSID ac:a3:1e:57:82:50 Profiles
-----
Profile Type                      Profile      Source
-----
802.11k Profile                  default     wlan virtual-ap "deauth_all"
dot11k-profile
RRM IE Profile                   default     wlan dot11k-profile "default"
rrm-ie-profile
Beacon Report Request Profile    default     wlan dot11k-profile "default"
bcn-rpt-req-profile
TSM Report Request Profile       default     wlan dot11k-profile "default"
tsm-req-profile
SSID Profile                     deauth_all  wlan virtual-ap "deauth_all"
ssid-profile
High-throughput SSID profile     default     wlan ssid-profile "deauth_all"
ht-ssid-profile

```

```

Advertisement Profile          default          wlan hotspot hs2-profile
"default" advertisement-profile
Hotspot 2.0 Profile          default          wlan virtual-ap "deauth_all"
hs2-profile
Virtual AP profile           deauth_all      ap-group "deauth_all" virtual-
ap
AAA Profile                   zren-1x-auth   wlan virtual-ap "deauth_all"
aaa-profile
AP "ac:a3:1e:cd:78:24" Radio 1 Profiles
-----
Profile Type                  Profile         Source
-----
802.11g radio profile        default        ap-group "deauth_all"
dot11g-radio-profile
Adaptive Radio Management (ARM) profile default-g      rf dot11g-radio-profile
"default" arm-profile
High-throughput radio profile default-g      rf dot11g-radio-profile
"default" ht-radio-profile
Spectrum profile            default-g      rf dot11g-radio-profile
"default" spectrum-profile
AM Scanning profile          default        rf dot11g-radio-profile
"default" am-scan-profile
AP "ac:a3:1e:cd:78:24" BSSID ac:a3:1e:57:82:40 Profiles
-----
Profile Type                  Profile         Source
-----
802.11k Profile              default        wlan virtual-ap "deauth_all"
dot11k-profile
RRM IE Profile               default        wlan dot11k-profile "default"
rrm-ie-profile
Beacon Report Request Profile default        wlan dot11k-profile "default"
bcn-rpt-req-profile
TSM Report Request Profile   default        wlan dot11k-profile "default"
tsm-req-profile
SSID Profile                 deauth_all     wlan virtual-ap "deauth_all"
ssid-profile
High-throughput SSID profile default        wlan ssid-profile "deauth_all"
ht-ssid-profile
Advertisement Profile          default        wlan hotspot hs2-profile
"default" advertisement-profile
Hotspot 2.0 Profile          default        wlan virtual-ap "deauth_all"
hs2-profile
Virtual AP profile           deauth_all      ap-group "deauth_all" virtual-
ap
AAA Profile                   zren-1x-auth   wlan virtual-ap "deauth_all"
aaa-profile
AP "ac:a3:1e:cd:78:24" Ethernet 0 Profiles
-----
Profile Type                  Profile         Source
-----
AP Ethernet Link profile     default        ap wired-port-profile "default" enet-
link-profile
AP LLDP Profile              default        ap wired-port-profile "default" lldp-
profile
AP wired port profile        default        ap-group "deauth_all" enet0-port-profile
AP "ac:a3:1e:cd:78:24" Ethernet 1 Profiles

```

```

-----
Profile Type          Profile  Source
-----
AP Ethernet Link profile  default  ap wired-port-profile "default" enet-
link-profile
AP LLDP Profile          default  ap wired-port-profile "default" lldp-
profile
AP wired port profile    default  ap-group "deauth_all" enet1-port-profile
AP "ac:a3:1e:cd:78:24" Ethernet 1 Wired AP Profiles
-----
Profile Type          Profile  Source
-----
Wired AP profile        default  ap wired-port-profile "default" wired-ap-
profile
AP wired port profile    default  ap-group "deauth_all" enet1-port-profile
AP "ac:a3:1e:cd:78:24" Ethernet 2 Profiles
-----
Profile Type          Profile  Source
-----
AP Ethernet Link profile  default  ap wired-port-profile "shutdown" enet-
link-profile
AP LLDP Profile          default  ap wired-port-profile "shutdown" lldp-
profile
AP wired port profile    shutdown  ap-group "deauth_all" enet-usb-port-
profile
AP "ac:a3:1e:cd:78:24" Ethernet 2 Wired AP Profiles
-----
Profile Type          Profile  Source
-----
Wired AP profile        default  ap wired-port-profile "shutdown" wired-ap-
profile
AP wired port profile    shutdown  ap-group "deauth_all" enet-usb-port-profile

```

Related Command

Command	Description
ap wired-ap-profile	This command configures a wired AP profile.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output was modified to display the list of profiles associated to Radio 2 in AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap provisioning

```
show ap provisioning {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{wired-mac <wired-mac>}
```

Description

This command shows provisioning parameters currently used by an AP.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific BSSID on an AP. An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Show data for an AP with a specific IPv6 address.
wired-mac <wired-mac>	Show data for an AP with a specific MAC address.

Example

The following example shows that the AP named AP8 has mostly default parameters. These appear with the value N/A.

```
(host) #show ap provisioning ap-name AP8
AP "mp2" Provisioning Parameters
-----
Item                               Value
----                               -
                                    

(host) (config) #show ap provisioning ap-name 00:24:6c:c7:d5:c8
AP "00:24:6c:c7:d5:c8" Provisioning Parameters
-----
Item                               Value
----                               -
AP Name                             00:24:6c:c7:d5:c8
AP Group                             default
Location name                         N/A
SNMP sysLocation                       N/A
Master/Conductor                       10.4.62.9
Gateway                               N/A
IPv6 Gateway                           N/A
Netmask                                N/A
```



```

IP Addr N/A
IPv6 Addr N/A
IPv6 Prefix 64
DNS IP N/A
DNS IPv6 N/A
Domain Name N/A
Server Name aruba-
master/conductor
Server IP 10.4.62.9
Antenna gain for 802.11a N/A
Antenna gain for 802.11g N/A
Antenna for 802.11a both
Antenna for 802.11g both
Single chain mode for Radio 0 0
Single chain mode for Radio 1 0
IKE PSK N/A
PAP User Name N/A
PAP Password N/A
PPPOE User Name N/A
PPPOE Password N/A
PPPOE Service Name N/A
PPPOE CHAP Secret N/A
USB User Name N/A
USB Password N/A
USB Device Type any
...
...
...

```

The output of this command includes the following parameters:

Column	Description
AP Name	Name of the AP.
AP Group	AP group to which the AP belongs.
Location name	FQLN for the AP.
SNMP sysLocation	User-defined description of the location of the AP, as defined with the command provision-ap syslocation.
Master/Conductor	Name or IP address for Mobility Conductor.
Gateway	IP address of the default gateway for the AP.
Netmask	Netmask for the AP's IP address.
IP Addr	IP address for the AP.
IPv6	The static IP6 address of the AP.6

Column	Description
IPv6 Prefix	The prefix of static IPv6 address of the AP.
Dns IP	IP address of the DNS server.
DNS IPv6	The prefix of static IPv6 address of the AP.
Domain Name	Domain name used by the AP.
Server Name	DNS name of the managed device from which the AP boots.
Server IP	IP address of the managed device from which the AP boots
Antenna gain for 802.11a	Antenna gain for 802.11a (5GHz) antenna.
Antenna gain for 802.11g	Antenna gain for 802.11g (2.4GHz) antenna.
Antenna for 802.11a	Antenna use for 5 GHz (802.11a) frequency band. <ul style="list-style-type: none"> ■ 1: AP uses antenna 1 ■ 2: AP uses antenna 2 ■ both: AP uses both antennas
Antenna for 802.11g	Antenna use for 2.4 GHz (802.11g) frequency band. <ul style="list-style-type: none"> ■ 1: AP uses antenna 1 ■ 2: AP uses antenna 2 ■ both: AP uses both antennas
Single chain mode for Radio 0	If this parameter is set to 1 for an 802.11n-capable radio, the radio will operate in single-chain mode, and will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This parameter is set to 0 (disabled) by default.
Single chain mode for Radio 1	If this parameter is set to 1 for an 802.11n-capable radio, the radio will operate in single-chain mode, and will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This parameter is set to 0 (disabled) by default.
IKE PSK	IKE PSK The IKE pre-shared key.
PAP password	Password Authentication Protocol (PAP) password for the AP.
PAP User Name	PAP username for the AP.
PPPOE User Name	Point-to-Point Protocol over Ethernet (PPPoE) user name for the AP.
PPPOE Password	PPPoE password for the AP.
PPPOE Service Name	PPPoE service name for the AP.

Column	Description
PPPOE CHAP secret	PPPoE CHAP secret key for the AP.
USB User Name	The PPP username provided by the cellular service provider
USB Password	A PPP password, if provided by the cellular service provider
USB Type	The USB driver type.
USB Device Identifier	The USB device identifier.
USB Dial String	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB Initialization String	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB TTY device data path	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
USB TTY device control path	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.
Uplink VLAN	If you configured an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature.
Link Priority Ethernet	Set the priority of the wired uplink, from 0-255. Each uplink type has an associated priority; wired ports having the highest priority by default.
Link Priority Cellular	The priority of the cellular uplink, from 0-255. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link.
Mesh Role	If the mesh role is "none," the AP is operating as a thin AP. An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
Installation	Indicates the type of installation (indoor or outdoor). The <code>default</code> parameter indicates that the installation mode is determined by the AP model type.
Latitude	Latitude coordinates of the AP, in the <i>Degrees Minutes Seconds</i> (DMS) format.
Longitude	Longitude coordinates of the AP, in the <i>Degrees Minutes Seconds</i> (DMS) format.

Column	Description
Altitude	Altitude, in meters, of the AP. This parameter is supported on outdoor APs only.
Antenna bearing for 802.11a	Horizontal coverage distance of the 802.11a (5GHz) antenna from true north, from 0-360 degrees. NOTE: This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
Antenna bearing for 802.11g	Horizontal coverage distance of the 802.11g (2.4GHz) antenna from true north, from 0-360 degrees. NOTE: This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
Antenna tilt angle for 802.11a	The angle of the 802.11a (5GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
Antenna tilt angle for 802.11g	The angle of the 802.11g (2.4GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
Mesh SAE	Shows if the AP has enabled or disabled Secure Attribute Exchange (SAE) on a mesh network.

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap provisioning-profile

```
show ap provisioning-profile [<profile-name>]
```

Description

This command shows information for AP provisioning profiles. The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group via the command `ap-group <group> provisioning-profile <profile>`.

Issue this command without the **<profile-name>** option to display the entire AP provisioning profile list, including profile status and the number of references to each profile. Include a profile name to display the authorization group defined for that profile.

Parameter	Description
<profile-name>	The name of an existing AP provisioning profile.

Examples

The following example lists all AP provisioning profiles. The **References** column lists the number of other profiles with references to that provisioning profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined AP provisioning profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] #show ap provisioning-profile

Provisioning profile List
-----
Name       References  Profile Status
----       -
default    12
outdoor    3
```

To display the configuration settings for an individual profile, include the <profile> parameter. The following example shows the profile details for the AP provisioning profile **Default**:

```
(host) [mynode] #show ap provisioning-profile default

Provisioning profile "default"
-----
Parameter                                     Value
-----
Remote-AP                                     No
```

```

Master/Conductor IP/FQDN
N/A
PPPOE User Name N/A
PPPOE Password N/A
PPPOE Service Name N/A
USB User Name N/A
USB Password N/A
USB Device Type none
USB Device Identifier N/A
USB Dial String N/A
USB Initialization String N/A
USB TTY device data path N/A
USB TTY device control path N/A
USB modeswitch parameters N/A
Link Priority Ethernet 0
Link Priority Cellular 0
Cellular modem network preference auto
Username of AP so that AP can authenticate to 802.1X using PEAP N/A
Password of AP so that AP can authenticate to 802.1X using PEAP N/A
Enable AP to 802.1x using EAP-TLS Disabled
Enable AP to use factory certificates when doing 802.1x EAP-TLS Disabled
AP dot1x EAP-TLS username suffix Enabled
AP dot1x EAP-TLS username suffix domain google.com
Uplink VLAN 0
USB power mode auto
AP POE Power optimization false
Master/Conductor Preference
IPv4

```

The output of this command includes the following parameters:

Parameter	Description
Remote-AP	Indicates that the profile is associated with a remote AP using certificates.
Master/Conductor IP/FQDN	The FQDN or IP address for Mobility Conductor.
PPPOE User Name	PPPoE username for the AP.
PPPOE Password	PPPoE password for the AP.
PPPOE Service Name	PPPoE service name for the AP.

Parameter	Description
USB User Name	The PPP username provided by the cellular service provider
USB Password	A PPP password, if provided by the cellular service provider
USB Device Type	The USB driver type.
USB Device Identifier	The USB device identifier.
USB Dial String	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB Initialization String	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB TTY device data path	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
USB TTY device control path	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.

Parameter	Description
USB modeswitch parameters	All the parameters that is required to be passed to the USB mode switch utility.
Link Priority Ethernet	Set the priority of the wired uplink, from 0-255. Each uplink type has an associated priority; wired ports having the highest priority by default.
Link Priority Cellular	The priority of the cellular uplink, from 0-255. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link.
Cellular modem network preference	Multi-mode cellular modem network preference type.
Username of AP so that AP can authenticate to 802.1X using PEAP	If your AP uses PEAP authentication, this field displays the AP username.
Password of AP so that AP can authenticate to 802.1X using PEAP	If your AP uses PEAP authentication, this field displays the AP password.
Enable AP to 802.1x using EAP-TLS	Enables AP to perform 802.1x authentication using EAP-TLS.

Parameter	Description
Enable AP to use factory certificates when doing 802.1x EAP-TLS	Enables AP to use the factory certificates to perform 802.1x EAP-TLS authentication.
AP dot1x EAP-TLS username suffix	Enables AP to use EAP-TLS username suffix.
AP dot1x EAP-TLS username suffix domain	Sets the suffix domain for AP dot1x EAP-TLS username. If defined, use EAP-TLS username as suffix, else use aruba.ap .
Uplink VLAN	If you configured an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature.
USB power mode	The USB power mode to control the power to the USB port.
AP POE Power optimization	Displays the AP POE power optimization status.
Master/Conductor Preference	Displays the preferred IP protocol for AP master /conductor discovery.

Related Command

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.7.0.0	The <code>Master Preference</code> parameter was added to the output of the <code>show ap-provisioning profile</code> command.
ArubaOS 8.4.0.0	The following parameters were added to the output of the <code>show ap-provisioning profile</code> command: <ul style="list-style-type: none">■ <code>AP dot1x EAP-TLS username suffix</code>■ <code>AP dot1x EAP-TLS username suffix domain</code>■ <code>USB power mode</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap provisioning-rule

```
show ap provisioning-rule [<profile-name>]
```

Description

This command displays information for an AP provisioning rule. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	The name of an existing AP provisioning rule.

Example

The following example shows the details of the conditions and actions for the AP provisioning rule: **test**:

```
(host) [mm] (config) #show ap provisioning-rule test

ap provisioning rule "test"
-----
Parameter                               Value
-----
ip range                                 N/A
network                                 3.3.3.3/1
any AP                                   false
AP Type                                  AP-UNKNOWN
ap group                                  N/A
Antenna gain for 802.11g                 N/A
Antenna gain for 802.11a                 N/A
Radio 0 5GHz Antenna gain for APs support Dual 5GHz mode N/A
Radio 1 5GHz Antenna gain for APs support Dual 5GHz mode N/A
```

The output of this command includes the following parameters:

Parameter	Description
ip range	Indicates the IPv4 or IPv6 address range to check if the IP address of the AP is within this range.

Parameter	Description
network	Specifies the IPv4 or IPv6 network address to check if the IP address of the AP is within this network address.
any AP	Indicates if you want to apply the provisioning rule's condition to any AP.
AP Type	Indicates the AP model to apply the rule to this particular AP.
ap group	Indicates the AP group that you want to assign to the AP.
Antenna gain for 802.11g	Indicates the antenna gain for 802.11g (2.4 GHz) antenna.
Antenna gain for 802.11a	Indicates the antenna gain for 802.11a (5 GHz) antenna.
Radio 0 5GHz Antenna gain for APs support Dual 5GHz mode	Antenna gain for radio 0 (5 GHz) antenna. This parameter is only displayed for APs that support dual 5 GHz mode.
Radio 1 5GHz Antenna gain for APs support Dual 5GHz mode	Antenna gain for radio 1 (5 GHz) antenna. This parameter is only displayed for APs that support dual 5 GHz mode.

Related Command

Command	Description
ap provisioning-rule	This command defines the conditions to select a group of APs and the subsequent actions to provision the APs.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap provisioning-rules

show ap provisioning-rules

Description

This command shows information for the priority level of AP provisioning rules. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the details of the conditions and actions for the AP provisioning rules:

```
(host) [mm] (config) #show ap provisioning-rules
ap provisioning rules
-----
Parameter                Value
-----
Provisioning Rule        ap324 priority 1
Provisioning Rule        ip36 priority 3
Provisioning Rule        network priority 5
Provisioning Rule        ip46 priority 7
```

Related Command

Command	Description
ap provisioning-rules	This command defines the priority of the provisioning rules that are actively used to auto-provision the APs.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap radio-database

```
show ap radio-database
  band [a|g] (For versions prior to ArubaOS 8.9.0.0)
  band [2.4GHz|5GHz|6GHz] (ArubaOS 8.9.0.0 or later versions)
  group <group>
  mode [access-point|air-monitor|disabled|ht|ht-40mhz|legacy|sap-monitor]
  page <page>
  sort-by [ap-group|ap-ip|ap-name|ap-type|switch-ip]
  sort-direction [ascending|descending]
  start <start>
  switch <switch-ip-addr>
```

Description

Show radio information for Access Points visible to this controller.

Parameter	Description
band	Show only APs with a radio operating in the specified band.
a (For versions prior to ArubaOS 8.9.0.0)	Show only APs with a radio operating in the 802.11a band (5 GHz).
g (For versions prior to ArubaOS 8.9.0.0)	Show only APs with a radio operating in the 802.11g band (2.4 GHz).
2.4GHz (ArubaOS 8.9.0.0 or later versions)	Show only APs with a radio operating in the 2.4 GHz band.
5GHz (ArubaOS 8.9.0.0 or later versions)	Show only APs with a radio operating in the 5 GHz band.
6GHz (ArubaOS 8.9.0.0 or later versions)	Show only APs with a radio operating in the 6 GHz band.
group <group>	Show only APs associated with the specified AP group.
mode	Show only APs with a radio operating in the specified mode.
access-point	Show only APs operating as access points.
air-monitor	Show only APs operating as air monitors.
disabled	Show only disabled APs.
ht	Show only high-throughput APs.

Parameter	Description
ht-40mhz	Show only 40 Mhz high-throughput APs.
legacy	Show only legacy (not high-throughput) APs.
sap-monitor	Show only APs operating as SAP monitors.
page <page>	Shows the number of APs.
sort-by	Sort the output of this command by a specific data column.
ap-group	Sort the output of this command by AP group name.
ap-ip	Sort the output of this command by AP IP address.
ap-name	Sort the output of this command by AP name.
ap-type	Sort the output of this command by AP model type.
switch-ip	Sort the output of this command by controller ip address.
sort-direction	Select a sort direction for the output of this command.
ascending	Sort the output in ascending order.
descending	Sort the output in descending order.
start	Start displaying the output of this command at a chosen index number by entering the index number of the AP at which command output should start.
switch <switch-ip-addr>	Display information for APs associated with a specific controller by entering the IP address of that controller.

Example

The following example shows the radio information for APs (For versions prior to ArubaOS 8.9.0.0).

```
(host) #show ap radio-database
AP Radio Database
```

```

-----
Name          Group      AP Type  IP Address  Status      Flags  Switch
IP
-----
-----
Radio 0 Band Ch/EIRP/MaxEIRP/Clients  Radio 1 Band Ch/EIRP/MaxEIRP/Clients
-----
Radio 2 Band Ch/EIRP/MaxEIRP/Clients
-----

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST; 1- =
802.1x use factory cert; 2 = Using IKE version 2
B = Built-in AP; C = Cellular RAP; D = Dirty or no config
E = Regulatory Domain Mismatch; F = AP failed 802.1x authentication
G = No such group; I = Inactive; J = USB cert at AP; L = Unlicensed
M = Mesh node
N = Duplicate name; P = PPPoe AP; R = Remote AP; R- = Remote AP requires
Auth;
S = Standby-mode AP; U = Unprovisioned; X = Maintenance Mode
Y = Mesh Recovery
c = CERT-based RAP; e = Custom EST cert; f = No Spectrum FFT support
i = Indoor; o = Outdoor; s = LACP striping; u = Custom-Cert RAP; z =
Datazone AP
p = In deep-sleep status
4 = WiFi Uplink
r = Power Restricted; T = Thermal ShutDown
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

```

The following example shows the radio information for APs, four of which are active (ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap radio-database

AP Radio Database
-----
Name          Group      AP Type  IP Address  Status      Flags
Switch IP    Standby IP  Radio 0 Band/Chan/HT-Type/EIRP  Radio 1
Band/Chan/HT-Type/EIRP  Radio 2 Band/Chan/HT-Type/EIRP
-----
-----
-----
ap215-12      default  215      1.1.1.5     Down        Rc2
10.65.47.6   0.0.0.0   N/A      N/A
N/A
ap325-12      default  325      10.65.47.59 Denied      N/A
10.65.47.6   0.0.0.0   N/A      N/A
N/A
ap335-12      default  335      10.65.47.60 Down        2
10.65.47.6   0.0.0.0   N/A      N/A
N/A
bc:9f:e4:c8:62:14 default  535      10.65.47.30 Down        2
10.65.47.6   0.0.0.0   N/A      N/A
N/A

```

```

cw-225          default 225      1.1.1.17      Down          Rc2
10.65.47.6 0.0.0.0      N/A          N/A
N/A
hhm-535          default 535      1.1.1.5      Up 43d:4h:19m:44s Rc2rID
10.65.47.6 0.0.0.0      AP:Unknown/18.0 Disabled
N/A
hhm-635          hhm-635 635      10.65.36.220 Up 20d:22h:15m:7s 2
10.65.47.6 0.0.0.0      Disabled Disabled
AP:6GHz/37S/HE/15.0
hhm-ap325        default 325      10.65.36.150 Up 20d:23h:16m:1s 2ID
10.65.47.6 0.0.0.0      AP:Unknown/0.0 Disabled
N/A
hhm-ap555        default 555      1.1.1.10     Down          Rc2
10.65.47.6 0.0.0.0      N/A          N/A
N/A
qc-225          default 225      1.1.1.4      Up 20d:23h:2m:49s Rc2
10.65.47.6 0.0.0.0      AP:5GHz/52E/VHT/18.0 Disabled
N/A
wli555          default 555      10.65.36.137 Down          2
10.65.47.6 0.0.0.0      N/A          N/A
N/A

Flags: 1 = 802.1x authenticated AP use EAP-PEAP; 1+ = 802.1x use EST;
1- = 802.1x use factory cert
      2 = Using IKE version 2; 4 = WiFi Uplink
      B = Built-in AP; C = Cellular RAP; D
= Dirty or no config
      E = Regulatory Domain Mismatch; F = AP failed 802.1x
authentication
      G = No such group; I = Inactive; J = USB cert at AP; L
= Unlicensed
      M = Mesh node
      N = Duplicate name; P = PPPoe AP; R = Remote AP;
R- = Remote AP requires Auth
      S = Standby-mode AP; T = Thermal ShutDown; U = Unprovisioned;
X = Maintenance Mode
      Y = Mesh Recovery
      b = bypass of AP1x timeout; c = CERT-based RAP; e = Custom EST
cert; f = No Spectrum FFT support
      i = Indoor; o = Outdoor; l = LAG
802.3ad; m = Protocol Mismatch
      p = In deep-sleep status; r = Power Restricted; s = LACP
striping; t = Temperature Restricted
      u = Custom-Cert RAP; z = Datazone AP

" Spectrum " followed by "^" indicates Local Spectrum Override in effect.

Total APs:11

```

The output of this command includes the following parameters:

Column	Description
Name	Name of the AP.
Group	AP group to which the AP is associated.
AP Type	AP model type.
IP address	IP address of the AP.
Status	Current AP status. If the AP is currently up, this data column also shows the amount of time for which the AP has been active.
Flags	This column displays a letter that corresponds to some type of additional information for the AP. The key to the list of possible flags appears at the bottom of the output of this command.
Switch IP	IP address of the AP's controller.
Standby IP (ArubaOS 8.9.0.0 or later versions)	Standby IP address of the AP's controller.
Radio 0 Band Ch/EIRP/MaxEIRP/Clients 8.9.0.0) (For versions prior to ArubaOS	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.

Column	Description
Radio 1 Band Ch/EIRP/MaxEIRP/Clients 8.9.0.0) (For versions prior to ArubaOS	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.
Radio 2 Band Ch/EIRP/MaxEIRP/Clients 8.9.0.0) (For versions prior to ArubaOS	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 2.
Radio 0 Band/Chan/HT-Type/EIRP (ArubaOS 8.9.0.0 or later versions)	Radio ID, band, channel, high-throughput traffic type, and EIRP of Radio 0.
Radio 1 Band/Chan/HT-Type/EIRP (ArubaOS 8.9.0.0 or later versions)	Radio ID, band, channel, high-throughput traffic type, and EIRP of Radio 1.
Radio 2 Band/Chan/HT-Type/EIRP (ArubaOS 8.9.0.0 or later versions)	Radio ID, band, channel, high-throughput traffic type, and EIRP of Radio 2.

Command History

Command	Description
ArubaOS 8.9.0.0	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ■ Replaced <code>band [a g]</code> with <code>band [2.4GHz 5GHz 6GHz]</code> parameters (ArubaOS 8.9.0.0 or later versions). ■ Replaced <code>Radio 0 Band Ch/EIRP/MaxEIRP/Clients</code> with <code>Radio 0 Band/Chan/HT-Type/EIRP</code> in the output parameter (ArubaOS 8.9.0.0 or later versions). ■ Replaced <code>Radio 1 Band Ch/EIRP/MaxEIRP/Clients</code> with <code>Radio 1</code>

Command	Description
	<p>Band/Chan/HT-Type/EIRP in the output parameter (ArubaOS 8.9.0.0 or later versions).</p> <ul style="list-style-type: none"> ■ Replaced Radio 2 Band <p>Ch/EIRP/MaxEIRP/Clients with Radio 2</p> <p>Band/Chan/HT-Type/EIRP in the output parameter (ArubaOS 8.9.0.0 or later versions).</p>
ArubaOS 8.6.0.0	<p>A new output parameter Radio 2 Band</p> <p>Ch/EIRP/MaxEIRP/Clients was introduced for AP-555 access points.</p>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap radio-summary

```
show ap radio-summary
  ap-group <ap-group>
  ap-name <ap-name>
  dot11a (For versions prior to ArubaOS 8.9.0.0)
  dot11g (For versions prior to ArubaOS 8.9.0.0)
  2.4GHz (ArubaOS 8.9.0.0 or later versions)
  5GHz (ArubaOS 8.9.0.0 or later versions)
  6GHz (ArubaOS 8.9.0.0 or later versions)
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

Show AP radios registered to this controller.

Parameter	Description
ap-group	Allows you to filter radio information by AP group.
ap-name <ap-name>	Allows you to filter radio information by AP name.
dot11a (For versions prior to ArubaOS 8.9.0.0)	Allows you to filter 802.11a radio information.
dot11g (For versions prior to ArubaOS 8.9.0.0)	Allows you to filter 802.11g radio information.
2.4GHz (ArubaOS 8.9.0.0 or later versions)	Allows you to filter 2.4 GHz radio information.
5GHz (ArubaOS 8.9.0.0 or later versions)	Allows you to filter 5 GHz radio information.
6GHz (ArubaOS 8.9.0.0 or later versions)	Allows you to filter 6 GHz radio information.
ip-addr <ip-addr>	Allows you to filter radio information by IP address.
ip6-addr <ip6-addr>	Allows you to filter radio information by IPv6 address.

Example

The output of the command in the following example displays statistics for the AP's radio, as well as statistics for transmitted and received frames.

In the actual CLI, it will appear in a single, long table.

```
(host) [mynode] #show ap radio-summary
APs Radios information
-----
Name                Group                AP Type  IP Address          Band  Mode
-----
172.17.153-7        172.17.153          104      55.55.57.44        2.4   AP:1
172.17.150-5        172.17.150          104      55.55.57.42        2.4   AP:6
172.17.153-13       172.17.153          104      55.55.57.35        2.4   AP:6
172.17.151-42       172.17.151          104      55.55.57.34        2.4   AP:11
172.17.151-34       172.17.151          104      55.55.57.33        2.4   AP:11
172.17.155-26       172.17.155          104      55.55.57.22        2.4   AP:1

EIRP/MaxEIRP      NF/U/I              TD                TM                TC
-----
28/29.5            -96/ 67/ 5          0/0/0/0/0/0      33/33/33/32/32/32 0/0/0/0/0/0
29.5/29.5          -96/ 27/ 3          0/0/0/0/0/0      12/11/12/12/12/11 0/0/0/0/0/0
29.5/29.5          -96/ 31/ 3          0/0/0/0/0/0      13/13/14/14/12/14 0/0/0/0/0/0
25/29.5            -96/ 28/ 6          0/0/0/0/0/0      10/10/10/9/11/10  0/0/0/0/0/0
25/29.5            -96/ 32/ 7          0/0/0/0/0/0      10/11/11/10/11/11 0/0/0/0/0/0
28/29.5            -96/ 70/ 4          0/0/0/0/0/0      27

NF: Noise Floor(dBm); U: Utilization(%); I: Interference(%)
TD: Time used by data frames (%); TM: time used by mgnt frames(%); time used
by ctrl frames (%)
Total Radios:6
```

The output of this command includes the following information:

Parameter	Description
Name	Name of the AP.
Group	Group to which AP radio is assigned.
AP Type	AP model.
IP Address	Radio IP address.
Band	Band on which radio is operating on (2.4 GHz or 5 GHz) (For versions prior to ArubaOS 8.9.0.0)/2.4 GHz, 5 GHz, or 6 GHz (ArubaOS 8.9.0.0 or later versions).
Mode	Mode on which radio is operating; AP: AP Mode; AM: Air Monitor Mode, Spectrum: Spectrum Monitor Mode. Optionally, you can also specify the channel number.
EIRP/Max EIRP	Current EIRP output and maximum EIRP allowed for this radio (dBm).
NF/U/I	Noise Floor (dBm) / Utilization (%) / Interference (%).

Parameter	Description
TD	Time used by data frames (%).
TM	Time used by mgmt frames(%).
TC	Time used by ctrl frames (%).

Command History

Version	Modification
ArubaOS 8.9.0.0	<p>The following changes were made:</p> <ul style="list-style-type: none"> ■ Replaced <code>dot11a</code> and <code>dot11g</code> with <code>5GHz</code> and <code>2.4GHz</code> parameters respectively (ArubaOS 8.9.0.0 or later versions).. ■ Introduced <code>6GHz</code> parameter for Wi-Fi 6E APs (ArubaOS 8.9.0.0 or later versions). ■ Introduced 6GHz value for <code>Band</code> output parameter (ArubaOS 8.9.0.0 or later versions).
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap regulatory

show ap regulatory

Description

Shows the currently active Regulatory Cert.

Example

The example below shows the version of Regulatory Cert currently active on the controller.

```
(host) [mynode] #show ap regulatory
Regulatory Version :1.0_43859
```

Related Commands

Command	Description
ap regulatory-domain-profile	This command configures an AP regulatory domain profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap regulatory-domain-profile

show ap regulatory-domain-profile [<profile-name>]

Description

Show the list of regulatory domain profiles or the settings in an individual regulatory domain profile. Issue this command without the <profile> parameter to display the entire regulatory domain profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Show data for a specific regulatory domain profile.

Examples

The following example shows that the controller has three regulatory domain profiles. The **References** column lists the number of other profiles with references to the regulatory domain profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] # show ap regulatory-domain-profile
Regulatory Domain profile List
-----
Name                               References  Profile Status
----                               -
corp-channel-profile                8
default                             10
channel-test                          1.
```

The following example displays the configuration settings for the profile **corp-channel-profile**. The output of this command shows the profile's country code and the valid channel and channel pairs for that profile (For versions prior to ArubaOS 8.9.0.0).

```
host) [mynode] #show ap regulatory-domain-profile corp-channel-profile
Regulatory Domain profile "corp-channel-profile"
-----
Parameter                           Value
-----
Country Code                          US
Valid 802.11g channel                 1
Valid 802.11g channel                 6
Valid 802.11a channel                 36
Valid 802.11a channel                 40
Valid 802.11a channel                 44
```

```

Valid 802.11a channel          48
Valid 802.11a channel          149
Valid 802.11a channel          153
Valid 802.11g 40MHz channel pair N/A
Valid 802.11a 40MHz channel pair 36-40
Valid 802.11a 40MHz channel pair 44-48
Valid 802.11a 40MHz channel pair 149-153
Valid 802.11a 80MHz channel group 36-48
Valid 802.11a 80MHz channel group 52-64
Valid 802.11a 80MHz channel group 100-112
Valid 802.11a 80MHz channel group 116-128
Valid 802.11a 80MHz channel group 132-144
Valid 802.11a 80MHz channel group 149-161

```

The following example displays the configuration settings for the profile **reg-635** of a Wi-Fi 6E AP. The output of this command shows the profile's country code and the valid channel and channel pairs for that profile (For ArubaOS 8.9.0.0 or later versions).

```

(host) [mynode] (config) #show ap regulatory-domain-profile reg-635

Regulatory Domain profile "reg-635"
-----
Parameter                               Value
-----
Country Code                             US
UTB Filter Blocking Selection             6GHz
Valid 802.11g channel                     1
Valid 802.11g channel                     6
Valid 802.11g channel                     11
Valid 802.11a channel                     36
Valid 802.11a channel                     40
Valid 802.11a channel                     44
Valid 802.11a channel                     48
Valid 802.11a channel                     149
Valid 802.11a channel                     153
Valid 802.11a channel                     157
Valid 802.11a channel                     161
Valid 802.11a channel                     165
Valid 802.11g 40MHz channel pair          1-5
Valid 802.11g 40MHz channel pair          7-11
Valid 802.11a 40MHz channel pair          36-40
Valid 802.11a 40MHz channel pair          44-48
Valid 802.11a 40MHz channel pair          149-153
Valid 802.11a 40MHz channel pair          157-161
Valid 802.11a 80MHz channel group          36-48
Valid 802.11a 80MHz channel group          149-161
Valid 802.11a 160MHz channel group         36-64
Valid 6GHz channel                        1
Valid 6GHz channel                        5
Valid 6GHz channel                        9
Valid 6GHz channel                        13
Valid 6GHz channel                        17

```

```

Valid 6GHz channel          21
Valid 6GHz channel          25
Valid 6GHz channel          29
Valid 6GHz channel          33
Valid 6GHz channel          37
Valid 6GHz channel          41
Valid 6GHz 40MHz channel pair 1-5
Valid 6GHz 40MHz channel pair 9-13
Valid 6GHz 40MHz channel pair 17-21
Valid 6GHz 40MHz channel pair 25-29
Valid 6GHz 40MHz channel pair 33-37
Valid 6GHz 40MHz channel pair 41-45
Valid 6GHz 80MHz channel group 17-29
Valid 6GHz 80MHz channel group 33-45
Valid 6GHz 80MHz channel group 49-61
Valid 6GHz 80MHz channel group 65-77
Valid 6GHz 80MHz channel group 81-93
Valid 6GHz 80MHz channel group 97-109
Valid 6GHz 80MHz channel group 113-125
Valid 6GHz 160MHz channel group 1-29

```

Starting from ArubaOS 8.11.0.0, OOB scanning on 6 GHz bands can be configured using the **oob_switch** parameter. The following CLI output displays OOB scanning on 6 GHz bands enabled.

```

host) [mynode] (config) #show ap regulatory-domain-profile 6EGroupAM_rdp_ui

Regulatory Domain profile "6EGroupAM_rdp_ui"
-----
Parameter                               Value
-----
Country Code                             CA
UTB Filter Blocking Selection            6GHz
OOB 6GHz scanning for AP615              enabled
Valid 802.11g channel                    1
Valid 802.11g channel                    6
Valid 802.11g channel                    11
Valid 802.11a channel                    36
Valid 802.11a channel                    40
Valid 802.11a channel                    44
Valid 802.11a channel                    48
Valid 802.11a channel                    52
Valid 802.11a channel                    56
Valid 802.11a channel                    60
Valid 802.11a channel                    64
Valid 802.11a channel                    100
Valid 802.11a channel                    104
Valid 802.11a channel                    108
Valid 802.11a channel                    112
Valid 802.11a channel                    116
Valid 802.11a channel                    132
Valid 802.11a channel                    136
Valid 802.11a channel                    140
Valid 802.11a channel                    144
Valid 802.11a channel                    149

```

```

Valid 802.11a channel          153
Valid 802.11a channel          157
Valid 802.11a channel          161
Valid 802.11a channel          165
Valid 802.11g 40MHz channel pair 1-5
Valid 802.11g 40MHz channel pair 7-11
Valid 802.11a 40MHz channel pair 36-40
Valid 802.11a 40MHz channel pair 44-48
Valid 802.11a 40MHz channel pair 52-56
Valid 802.11a 40MHz channel pair 60-64
Valid 802.11a 40MHz channel pair 100-104
Valid 802.11a 40MHz channel pair 108-112
Valid 802.11a 40MHz channel pair 132-136
Valid 802.11a 40MHz channel pair 140-144
Valid 802.11a 40MHz channel pair 149-153
Valid 802.11a 40MHz channel pair 157-161
Valid 802.11a 80MHz channel group 36-48
Valid 802.11a 80MHz channel group 52-64
Valid 802.11a 80MHz channel group 100-112
Valid 802.11a 80MHz channel group 132-144
Valid 802.11a 80MHz channel group 149-161
Valid 802.11a 160MHz channel group 36-64
Valid 6GHz channel             N/A
Valid 6GHz 40MHz channel pair  N/A
Valid 6GHz 80MHz channel group N/A
Valid 6GHz 160MHz channel group N/A

```

The output of this command includes the following information:

Column	Description
Country Code	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum.

Column	Description
<p>UTB Filter Blocking Selection (For ArubaOS 8.9.0.0 or later versions)</p>	<p>This parameter displays the band on which the UTB limitation is applied in the regulatory-domainprofile. The utb filter supports channel band on both 5 GHz and 6 GHz. This parameter displays one of the following values:</p> <ul style="list-style-type: none"> ■ 5GHz—5 GHz for upper band blocking. ■ 6GHz—6 GHz for lower band blocking.
<p>OOB 6GHz scanning for AP-615</p>	<p>If enabled, OOB scanning on 6 GHz band is allowed. If disabled, OOB scanning on 6 GHz band is blocked. This switch is valid only for AP-615 access points in the 5GHz-and-2.4GHz operation mode. Disable the switch to enable the use of UNII-4 band. Default: Enabled.</p>

Column	Description
Valid 802.11g channel	Selected 802.11b/g channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the profile's country code.
Valid 802.11a channel	Selected 802.11a channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the country code.
Valid 802.11g 40MHz channel pair	Selected 802.11b/g 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
Valid 802.11a 40MHz channel pair	Selected 802.11a 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.

Column	Description
Valid 802.11a 80MHz channel group	Selected 802.11a 80 MHz channel group available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
Valid 6GHz channel (For ArubaOS 8.9.0.0 or later versions)	Selected 6 GHz channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the profile's country code.
Valid 6GHz 40MHz channel pair (For ArubaOS 8.9.0.0 or later versions)	Selected 6 GHz 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
Valid 6GHz 80MHz channel group (For ArubaOS 8.9.0.0 or later versions)	Selected 6 GHz 80 MHz channel group available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.

Column	Description
Valid 6GHz 160MHz channel group (For ArubaOS 8.9.0.0 or later versions)	Selected 6 GHz 160 MHz channel group available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.

Related Commands

Command	Description
ap regulatory-domain-profile	This command configures an AP regulatory domain profile.

Command History

Version	Modification
ArubaOS 8.11.0.0	The command output was modified to display OOB 6GHz scanning for AP-615 settings.
ArubaOS 8.9.0.0	The command output was modified to display the following new parameters (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> ■ UTB Filter Blocking Selection ■ Valid 6GHz channel ■ Valid 6GHz 40MHz channel pair ■ Valid 6GHz 80MHz channel group ■ Valid 6GHz 160MHz channel group
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote auth-trace-buf

```
show ap remote auth-trace-buf {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows authentication trace buffer on an AP.

Parameter	Description
ap-name <ap-name>	Shows authentication trace buffer on an AP for specified AP name.
bssid <bssid>	Shows authentication trace buffer on an AP for specified BSSID.
ip-addr <ip-addr>	Shows authentication trace buffer on an AP for specified IP address.
ip6-addr <ip6-addr>	Shows authentication trace buffer on an AP for specified IPv6 address.

Example

The following example shows authentication trace buffer on an AP named ap-205:

```
(host) [mynode] #show ap remote auth-trace-buf ap-name ap-205  
  
Auth Trace Buffer  
-----
```

Related Commands

Command	Description
aaa auth-trace	This command sets parameters for debug tracing in AUTH (light weight tracing).

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote blacklist-clients/show ap remote denylist -clients

```
show ap remote blacklist-clients/show ap remote denylist -clients [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>]
```

Description

This command shows all clients blacklisted/denylisted.

Parameter	Description
ap-name <ap-name>	Shows all blacklisted/denylisted clients filtered by AP name.
bssid <bssid>	Shows all blacklisted/denylisted clients filtered by BSSID.
ip-addr <ip-addr>	Shows all blacklisted/denylisted clients filtered by IP address.

Example

The following example shows all blacklisted/denylisted clients:

```
(host) [mynode] #show ap remote blacklist-clients ap-name ap-205

Blacklisted Clients
-----
STA  reason  block-time(sec)  remaining time(sec)  Flags
---  -
Flags: R: reject associations
```

Starting from ArubaOS 8.9.0.0, the output of the command is displayed as follows:

```
(host) [mynode] #show ap remote denylist-clients ap-name ap-205

Denylisted Clients
-----
STA  reason  block-time(sec)  remaining time(sec)  Flags
---  -
Flags: R: reject associations
```

Related Commands

Command	Description
stm add-blacklist-client /add-denylist-client	Manually add clients from a blacklist/denylist.
stm remove-blacklist-client/remove-denylist-client <macaddr>	Manually remove clients from a blacklist/denylist.
show ap blacklist-clients / show ap denylist-clients	Show a list of clients that have been denied access.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote blacklist-clients-driver / show ap remote denylist-clients-driver

```
show ap remote blacklist-clients-driver / show ap remote denylist-clients-driver  
[ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]
```

Description

This command shows all clients blacklisted/denylisted in the driver.

Parameter	Description
ap-name <ap-name>	Shows all clients blacklisted/denylisted in the driver filtered by AP name.
bssid <bssid>	Shows all clients blacklisted/denylisted in the driver filtered by BSSID.
ip-addr <ip-addr>	Shows all clients blacklisted/denylisted in the driver filtered by IP address.
ip6-addr <ip6-addr>	Shows all clients blacklisted/denylisted in the driver filtered by IPv6 address.

Example

The following example shows all clients blacklisted/denylisted in the driver:

```
(host) [mynode] #show ap remote blacklist-clients-driver ap-name ap-205  
  
Clients Blacklisted in Driver  
-----  
STA  
---
```

Starting from ArubaOS 8.9.0.0, the output of the command is displayed as follows:

```
(host) [mynode] # show ap remote denylist ap-name ap-205  
  
Clients Denylisted in Driver  
-----  
STA  
---
```

Related Commands

Command	Description
stm	This command is used to manually disconnect a client from an AP or control the denylisting of clients.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote bss-table

```
show ap remote bss-table [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>]  
[ip6-addr <ip6-addr>]
```

Description

This command shows BSSIDs of all APs registered on the managed device. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows BSSIDs of all APs registered on the managed device filtered by AP name.
bssid <bssid>	Shows BSSIDs of all APs registered on the managed device filtered by BSSID.
ip-addr <ip-addr>	Shows BSSIDs of all APs registered on the managed device filtered by IP address.
ip6-addr <ip6-addr>	Shows BSSIDs of all APs registered on the managed device filtered by IPv6 address.

Example

The following example shows the BSSID of an AP registered on the managed device (For versions prior to ArubaOS 8.9.0.0).

```
(host) [mynode] #show ap remote bss-table ap-name ap-205  
  
Aruba AP BSS Table  
-----  
bss                ess                port  ip                phy  
---                ---                ----  --                ---  
40:e3:d6:76:19:70  aruba-ap           ?/?   191.191.191.252  a-VHT  
40:e3:d6:76:19:71  guestthistime     ?/?   191.191.191.252  a-VHT  
40:e3:d6:76:19:60                ?/?   191.191.191.252  g-HT  
  
type  ch/EIRP/max-EIRP  cur-cl  ap name  in-t(s)  tot-t  
-----  
ap    149E/12/24        0       ap-205   0         19d:13h:46m:14s  
ap    149E/12/24        0       ap-205   0         19d:13h:46m:14s  
am    ?/?/?             0       ap-205   0         19d:13h:46m:13s  
  
Channel followed by "*" indicates channel selected due to unsupported  
configured channel.
```

"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:3
Num Associations:0

The following example shows the BSSID of a Wi-Fi 6E AP registered on the managed device (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] #show ap remote bss-table ap-name hhm-635

Aruba AP BSS Table
-----
bss          ess          port ip          band/ht-mode/bandwidth
ch/EIRP/max-EIRP  type  cur-cl  ap name  in-t(s)  tot-t          flags
---          ---          ---  --          --          -----
cc:88:c7:41:64:60 8@hhm-635-psk  ??    10.65.36.220 6GHz/HE/160MHz
37S/15.0/21.8    ap    0      hhm-635  0         20d:12h:34m:1s TWx3

Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:1
Num Associations:0

Flags:      a = Airslice policy; A = Airslice app monitoring; c = MBO
Cellular Data Capable BSS; d = Deferred Delete Pending; D = VLAN Discovered;
E = Enhanced-open BSS without transition mode; I = Imminent VAP Down; K =
802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS;
o = Enhanced-open transition mode open BSS; O = Enhanced-open BSS with
transition mode; r = 802.11r Enabled; t = Broadcast TWT Enabled;
T = Individual TWT Enabled; W = 802.11W Enabled; x = MBSSID Tx BSS; 3 = WPA3
BSS;
```

The output of this command includes the following information:

Column	Description
bss	The AP Basic Service Set Identifier (BSSID). This is usually the MAC address of the AP
ess	The AP Extended Service Set Identifier (ESSID).
port	The slot and port used by the controller, in the format <slot>/<module>/<port>.
ip	IP address of an AP.

Column	Description
phy (For versions prior to ArubaOS 8.9.0.0)	The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b or 802.11g, 802.11b or 802.11g-HT-20.
band/ht-mode/bandwidth (ArubaOS 8.9.0.0 or later versions)	The AP radio type displayed as radio band/throughput type/channel bandwidth. Possible values for each type are as follows: <ul style="list-style-type: none"> band—2.4GHz, 5GHz, or 6GHz ht-mode—HT, VHT, or HE bandwidth—20MHz, 40MHz, 80MHz, 80+80MHz, or 160MHz
ch/EIRP/max-EIRP	Radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.
type	Shows whether the AP is working as an access point (AP) or air monitor (AM).
cur-cl	Current number of clients on the AP.
ap name	Name of the AP.
in-t (s)	Number of seconds that an AP has been inactive.
tot-t	An AP's total active time, in seconds.
flags	The type of flags available for the AP.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the following: <ul style="list-style-type: none"> Replaced <code>phy</code> parameter with <code>band/ht-mode/bandwidth</code>. Added x and 3 flags.
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote client status

```
show ap remote client status [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] <client-mac>
```

Description

This command shows association state of clients. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows association state of clients filtered by AP name.
bssid <bssid>	Shows association state of clients filtered by BSSID.
ip-addr <ip-addr>	Shows association state of clients filtered by IP address.
ip6-addr <ip6-addr>	Shows association state of clients filtered by IPv6 address.
<client-mac>	MAC address of client.

Example

The following example shows association state of clients:

```
(host) [mynode] #show ap remote client status ap-name ap-205  
00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The ip6-addr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ap remote counters

```
show ap remote counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the numbers of message counters for Remote APs.

Parameter	Description
ap-name <ap-name>	Show data for an AP with a specific name.
bssid <bssid>	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address.
ip-addr <ip-addr>	Show data for an AP with a specific IP address.

Example

Use this command to determine the number of message counters recorded for each counter type seen by the remote AP. The output of the command in the example below shows counters for Remote AP State and VoIP CAC State Announcements:

```
(host) [mynode] #show ap remote counters ap-name a122

Counters
-----
Name                               Value
----                               -
Remote AP State                     62851
VoIP CAC State Announcement         13605
```

The output of this command includes the following information:

Column	Description
Name	Name of the counter type.
Value	Number of counters recorded since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap remote-debug-pkt

```
show ap remote-debug-pkt [logs|status] {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the packet debugging details of an AP.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
logs {ap-name <ap-name> ip-addr <ip-addr> ip6-addr <ip6-addr>}	Shows packet debugging logs.
status {ap-name <ap-name> ip-addr <ip-addr> ip6-addr <ip6-addr>}	Shows packet debugging status.

Example

The following command displays the packet debugging status of an AP.

```
(host) [mynode] #show ap remote-debug-pkt status ip-addr 10.82.113.45
Debug pkt status at AP655
-----
Dump is not started, run 'ap remote-debug-pkt dump start' to enable
Mirror is not started, run 'ap remote-debug-pkt mirror' to mirror them
```

```
Run 'ap remote-debug-pkt type' to config debug types
```

Command History

Version	Modification
ArubaOS 8.11.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on managed devices.

show ap remote debug anul-sta-entries

```
show ap remote debug anul-sta-entries {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Displays a list of VAPs and stations stored in the AP's datapath. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Show LACP information for an AP with a specific name.
radio <radio>	Shows the radio ID. Valid values are 0 and 1.
ip-addr <ip-addr>	Show LACP information for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Show LACP information for an AP with a specific IPv6 address.

Example

Using the following example, for 320 Series, check the LAG columns to see if any packets are dropped.

```
(host) [mynode] #show ap remote debug anul-sta-entries ap-name ap325
ANUL BSS Table for Radio 0
-----
bssid                num_stas  data ready drops
-----
AC:A3:1E:53:5C:F0    2          0
ANUL STA State
-----
mac                  bssid                aid  data ready  bss  Drops  LAG  LAG
drops
---                  ---                  ---  -----  ---  -----  ---  ----
-----
3C:A9:F4:24:B2:54    AC:A3:1E:53:5C:F0    2    Yes         B    0      Yes  0
78:31:C1:BC:D6:12    AC:A3:1E:53:5C:F0    1    Yes         B    0      Yes  0
```

The following parameters appear in the output of the `show ap remote debug anul-sta-entries` command and are useful for debugging purposes.

Parameter	Description
bssid	The BSSID of the VAP.
num_stas	Indicates the number of stations associated to a VAP.
data ready drops	Indicates the total packets received and dropped before clients were ready to receive data packets.
ANUL STA State	
mac	The MAC address of a client.
bssid	The BSSID of the VAP that the client is associated to.
aid	The association ID of the station.
data ready	Indicates if the client has completed authentication.
bss	Indicates if a client is associated to a BSS or not. The B flag indicates that the client is associated to a BSS. The F flag indicates that the entry is free and not attached to any BSS.
Drops	Indicates the number of data packets received and dropped before data ready is set to yes.
LAG	Indicates if link aggregation is used to achieve HT by transmitting the packets on both Ethernet ports, for a given station. This field is displayed only in 320 Series access points.
LAG drops	Indicates the number of packets dropped by the AP due to packets reordered in the network by link aggregation. This field is displayed only in 320 Series access points.

Command History

Version	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on managed devices.

show ap remote debug association

```
show ap remote debug association
  {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>} [uac
  <uac>]
```

Description

This command shows the association table of the AP to identify the clients associated to each AP. Use this command to verify if a remote user is connected to an AP and to validate the AP to which is connected. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows client associations for the specified AP name.
bssid <bssid>	Show client associations for an specific BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows client associations for the specified IP address.
ip6-addr <ip6-addr>	Shows client associations for the specified IPv6 address.

Example

The output of this command displays information about the remote clients associated with an AP with the IP address 192.0.2.32:

```
(host) [mynode] #show ap remote debug association ip-addr 192.0.2.32

Flags: W: WMM client, A: Active, R: RRM client

PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
             <n>ss: <n> spatial streams

Association Table
-----
Name  bssid                mac                auth  assoc  aid  l-int  essid
----  -
AP71  00:0a:23:c1:d4:11    00:16:6d:08:1s:f1  y     y     1   10     t-lab

vlan-id  tunnel-id  phy  assoc. time  num assoc  Flags
-----  -
111      0x108e    a

Num Clients:1
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.
bssid	The AP BSSID.
mac	MAC address of the client.
auth	This column displays a y if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an n .
assoc	This column displays a y if the AP has been configured for 802.11 association frame types. Otherwise, it displays an n .
aid	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
l-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's ESSID.
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
phy	The RF band in which the AP operates: <ul style="list-style-type: none"> ■ a = 5 GHz ■ b, g = 2.4 GHz From ArubaOS 8.9.0.0 or later versions, the following values are displayed: <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz (For Wi-Fi 6E APs)
assoc. time	Amount of time the client has associated with the AP, in the format hours:minutes:seconds.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the <code>show ap association</code> command.

Command History:

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the following values for <code>phy</code> parameter (For ArubaOS 8.9.0.0 or later versions): <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz (For Wi-Fi 6E APs)
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Configuration mode on managed devices.

show ap remote debug association-failure

```
show ap remote debug association-failure
  {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}[client-
  mac <client-mac>|ssid <ssid>]
```

Description

This command shows the association failure information.

Parameter	Description
ap-name <ap-name>	Shows AP association failure for the specified AP name. You may include the client-mac or ssid to filter the output.
bssid <bssid>	Shows AP associations for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Shows AP associations for the specified IP address. You may include the client-mac or ssid to filter the output.
ip6-addr <ip6-addr>	Shows AP associations for the specified IPv6 address. You may include the client-mac or ssid to filter the output.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command displays information about the association failure for an AP named **ap-205**:

```
(host) [mynode] #show ap remote debug association-failure ap-name ap-205

Association Failure Table
-----
MAC Address  AP Name  BSSID  ESSID  State  Radio  Idle Time  Reason
-----
Num Association Failures:0
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Configuration mode on managed devices.

show ap remote debug association-failure

```
show ap remote debug association-failure [{ap-name <ap-name>}|{bssid <bssid>}|{essid <essid>}]
```

Description

Display association failure information that can be used to troubleshoot problems on an AP. Use this command to determine whether the client is associated and identify the last AP to which it was connected.

Parameter	Description
ap-name <ap-name>	Filter the Association Failure Table by AP name.
bssid <bssid>	Filter the Association Failure Table by BSSID. The BSSID is usually the AP's MAC address.
essid <essid>	Filter the Association Failure Table by ESSID of an AP.

Example

The output of the command `show ap remote debug association-failure` displays the Association Failure Table. If the **Idle time** column in the output of this command is a low value, the **reason** column will describe why the association failed.

```
(host) [mynode] #show ap remote debug association-failure ap-name AP-65-
port3
Association Failure Table
-----
MAC Address      AP Name  BSSID                ESSID  State  Radio  Idle
Time    Reason
-----
---
00:16:6f:09:54:3e AL29      00:1a:1e:11:6f:00  guest                802.11g
20h:39m:33s Denied; AP Going Down
00:16:6f:09:54:3e AL33      00:1a:1e:11:6e:60  guest  auth    802.11g
20h:39m:33s Unspecified Failure
00:16:6f:09:54:3e AL40      00:1a:1e:8d:5b:20  guest                802.11g
20h:39m:33s Denied; Ageout
Num Association Failures:3
```

The output of this command includes the following parameters:

Column	Description
MAC address	MAC address of the client that failed to associate with an AP.
AP Name	Name of an AP to which the client attempted to associate.
BSSID	BSSID of an AP.
ESSID	ESSID of an AP.
State	This data column shows if the client is currently authorized or both authorized and ESSID associated with an AP.
Radio	The AP radio type.
Idle Time	Amount of time that the client has been idle, in the format <i>hours:minutes:seconds</i> .
Reason	A brief description of the reason why the client failed to associate.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap remote debug bss-config

```
show ap remote debug bss-config {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Shows the configuration for each BSSID of an AP. This information can be used to troubleshoot problems on an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Filter the AP Config Table by AP name.
bssid <bssid>	Shows AP associations for the specified BSSID. A BSSID is usually the MAC address of an AP.
ip-addr <ip-addr>	Filter the AP Config Table by IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Filter the AP Config Table by IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

The following example shows the AP configuration table for a specific BSSID (For versions prior to ArubaOS 8.9.0.0):

```
(host) [mynode] #show ap remote debug bss-config ap-name ap93-3
Aruba AP Config Table
bssid      ess      vlan ip      phy  type  fw-mode
max-cl  rates tx-rates  preamble  mtu
-----
-----
----- status  wmm
-----
00:1a:1e:11:24:c2  cera2  66  10.6.1.203  g-HT  ap  tunnel  64
0x3      0xffff  enable  0  enable  enable
00:1a:1e:8d:5b:11  wpa2   65  10.6.1.198  a-HT  ap  tunnel  20
0x150    0xff0   -      0  enable  enable
00:0b:86:9b:e5:60  guest  63  10.6.14.79  g      ap  tunnel  20
0x2      0x3fe  enable  0  enable  enable
00:1a:1e:97:e5:41  voip   66  10.6.1.199  g-HT  ap  tunnel  20
0xc      0x14c  enable  0  enable  enable
00:1a:1e:11:74:a1  voip   66  10.6.1.197  g-HT  ap  tunnel  20
0xc      0x14c  enable  0  enable  enable
```

```
00:1a:1e:11:5f:11  wpa2    65    10.6.1.200  a-HT  ap    tunnel  20
0x150 0xff0      -      0      enable  enable
```

The following example shows the AP configuration table for a specific BSSID on a Wi-Fi 6E AP (For ArubaOS 8.9.0.0 or later versions):

```
(host) [mynode] (config) #show ap remote debug bss-config ap-name hhm-635

Aruba AP Config Table
-----
bss          ess          vlan ip          band/ht-mode/bandwidth
type fw-mode  max-cl  rates tx-rates  preamble  status wmm      mtu
flags
---          ---          ----  --          -----
--
cc:88:c7:41:64:60 8@hhm-635-psk 1      10.65.36.220 6GHz/HE/160MHz
ap tunnel  64      0x150 0xff0  enable  enable  enable 1500
TWx3

Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:1
Num Associations:0

Flags:      a = Airslice policy; A = Airslice app monitoring; c = MBO
Cellular Data Capable BSS; d = Deferred Delete Pending; D = VLAN Discovered;
E = Enhanced-open BSS without transition mode; I = Imminent VAP Down; K =
802.11K Enabled; m = Agile Multiband (MBO) BSS; M = WPA3-SAE mixed mode BSS;
o = Enhanced-open transition mode open BSS; O = Enhanced-open BSS with
transition mode; r = 802.11r Enabled; t = Broadcast TWT Enabled;
T = Individual TWT Enabled; W = 802.11W Enabled; x = MBSSID Tx BSS; 3 = WPA3
BSS;
```

The output of this command includes the following information:

Column	Description
bss	BSS identifier, which is usually the AP's MAC address.
ess	ESS identifier; a user-defined name for a wireless network.
vlan	The BSSID VLAN number.
IP	The AP IP address.
phy	One of the following 802.11 types

Column	Description
(For versions prior to ArubaOS 8.9.0.0)	<ul style="list-style-type: none"> ■ a ■ a-HT ■ g ■ g-HT
band/ht-mode/bandwidth (ArubaOS 8.9.0.0 or later versions)	<p>The AP radio type displayed by radio band/throughput type/channel bandwidth. Possible values for each type are as follows:</p> <ul style="list-style-type: none"> ■ band—2.4GHz, 5GHz, or 6GHz ■ ht-mode—HT, VHT, or HE ■ bandwidth—20MHz, 40MHz, 80MHz, 80+80MHz, or 160MHz
type	This column shows if the BSSID is for an AP or an AM.
fw-mode	<p>The configured forward mode for the AP's virtual AP profile.</p> <ul style="list-style-type: none"> ■ bridge: Bridge locally ■ split-tunnel: Tunnel to controller or NAT locally ■ tunnel: Tunnel to controller
max-cl	The maximum number of clients allowed for this BSSID.
preamble	Shows if short preambles are enabled for 802.11b or 802.11g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using a short preamble.
MTU	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
status	Shows if this BSSID is enabled or disabled.
wmm	Shows if the BSSID has enabled or disabled WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF) WMM provides prioritization of specific traffic relative to other traffic in the network.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the following: <ul style="list-style-type: none"> Replaced <code>phy</code> parameter with <code>band/ht-mode/bandwidth</code>. Added x and 3 flags.
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on managed devices.

show ap remote debug bucketmap datapath

```
show ap remote debug bucketmap datapath {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} essid <essid>
```

Description

This command shows bucket maps in AP datapath.

Parameter	Description
ap-name <ap-name> essid <essid>	Shows bucket maps filtered by specified AP name and ESSID.
ip-addr <ip-addr> essid <essid>	Shows bucket maps filtered by specified IP address of an AP and ESSID.
ip6-addr <ip6-addr> essid <essid>	Shows bucket maps filtered by specified IPv6 address of an AP and ESSID.

Example

Access the CLI and use the following command to show bucket maps in AP datapath filtered by the AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap datapath ap-name test essid default

Essid default radio=0 zone=1 - Num UACs 4
-----
Index  ArrayIdx  UAC IP          Active AAC  Standby AAC  Num STAs
-----  -
0      0          10.15.146.3    Yes        No           0
1      1          10.15.146.4    No         No           1
2      2          10.15.146.5    No         No           0
3      3          10.15.146.6    No         No           0
Station List
-----
UAC Index  Station Mac      BSSID
-----  -
1          80:86:F2:40:14:8D  9C:1C:12:89:5C:9C
Bucket Map
-----
Bucket Idx Range  Bucket Map
-----  -
[0-31]            0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0
1 2 3
[32-63]           0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0
1 2 3
```



```

[64-95]          0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0
1 2 3
[96-127]         0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0
1 2 3
[128-159]        0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0
1 3 0
[160-191]        1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3
0 1 3
[192-223]        0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1
3 0 1
[224-255]        0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1
-               Standby Map
[0-31]           1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1
0 1 1
[32-63]          1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1
0 1 1
[64-95]          1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1
0 1 1
[96-127]         1 0 1 1 1 0 1 1 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3
0 0 0
[128-159]        3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3
0 0 3
[160-191]        0 0 3 0 0 3 0 0 3 0 0 3 0 0 3 0 2 3 3 2 3 3 2 3 3 2
3 3 2
[192-223]        3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3
2 3 3
[224-255]        3 3 3 3 3 3 3 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
2 2 2
Statistics:Bmap Updates=0; UAC:Adds=4 Deletes=0; STA:Adds=0 Deletes=494
moves=0 errs=0 copies=0

```

The following command shows bucket maps in AP datapath for AP-555 access points,

```

(host) [mynode] #show ap remote debug bucketmap datapath ap-name AP555-0
Essid triradio-D-Tunnel-Open radio=0,1,2 zone=0 - Num UACs 1
-----
Index  ArrayIdx  UAC IP          Active AAC      Standby AAC     Num STAs
-----
0      0            192.168.40.6   Yes             No              1
Station List
-----
UAC Index  Station Mac      BSSID
-----
0          D8:FC:93:48:C5:EC  80:8D:B7:80:BA:F0
Bucket Map
-----
Bucket Idx Range  Bucket Map
-----
[0-31]           0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0
0

```


Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable mode on managed devices.

show ap remote debug bucketmap sapd

```
show ap remote debug bucketmap sapd {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} essid <essid>
```

Description

This command shows bucket map received from cluster by SAPD process.

Parameter	Description
ap-name <ap-name> essid <essid>	Shows bucket maps received from cluster by SAPD filtered by specified AP name and ESSID.
ip-addr <ip-addr> essid <essid>	Shows bucket maps received from cluster by SAPD filtered by specified IP address of an AP and ESSID.
ip6-addr <ip6-addr> essid <essid>	Shows bucket maps received from cluster by SAPD filtered by specified IPv6 address of an AP and ESSID.

Example

Access the CLI and use the following command to show bucket map received from cluster by SAPD process filtered by AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap sapd ap-name test essid default
Bucket map for essid default (Rcvd at Tue May 31 16:29:08 2016 [19h:39m:41s ago]);gen_num=1
-----
-----
Item                               Value
----                               -
Essid                               default
UAC 0                               10.15.146.3
UAC 1                               10.15.146.4
UAC 2                               10.15.146.5
UAC 3                               10.15.146.6
Active Map [0-31]                   00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [32-63]                  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [64-95]                  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [96-127]                 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [128-159]                00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 03 00
```

```

Active Map [160-191]      01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03
Active Map [192-223]    00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
Active Map [224-255]    00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01

Standby Map [0-31]      01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [32-63]    01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [64-95]    01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [96-127]   01 00 01 01 01 00 01 01 03 00 00 00 03 00 00 00
03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00
Standby Map [128-159]  03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00
03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 03
Standby Map [160-191]  00 00 03 00 00 03 00 00 03 00 00 03 00 00 03 00
02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02
Standby Map [192-223]  03 03 02 03 02 03 02 03 03 02 03 03 02 03 03 02
03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03
Standby Map [224-255]  03 03 03 03 03 03 03 03 03 03 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02

L2 Connectedness [0-31]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [32-63]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [64-95]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [96-127]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [128-159]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [160-191]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [192-223]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1
L2 Connectedness [224-255]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable mode on managed devices.

show ap remote debug bucketmap stm

```
show ap remote debug bucketmap stm {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [essid <essid>]
```

Description

This command shows bucket map received from cluster by AP STM. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name> essid <essid>	Shows bucket map received from cluster by AP STM filtered by specified AP name and ESSID.
ip-addr <ip-addr> essid <essid>	Shows bucket map received from cluster by AP STM filtered by specified IP address of an AP and ESSID.
ip6-addr <ip6-addr> essid <essid>	Shows bucket map received from cluster by AP STM filtered by specified IPv6 address of an AP and ESSID.

Example

Access the CLI and use the following command to show bucket map received from cluster by AP STM filtered by AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap stm ap-name test essid default

Bucket map for essid default
-----
Item                               Value
----                               -
Essid                               default
UAC 0                              10.15.146.3 (Up)
UAC 1                              10.15.146.4 (Up)
UAC 2                              10.15.146.5 (Up)
UAC 3                              10.15.146.6 (Up)
Current Map [0-31]                  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Current Map [32-63]                 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Current Map [64-95]                 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
```

```

Current Map [96-127]      00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Current Map [128-159]    00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Current Map [160-191]    01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03
Current Map [192-223]    00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
Current Map [224-255]    00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01

Active Map [0-31]        00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [32-63]       00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [64-95]       00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [96-127]      00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [128-159]     00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [160-191]     01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03
Active Map [192-223]     00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
Active Map [224-255]     00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01

Standby Map [0-31]       01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [32-63]      01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [64-95]      01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01
Standby Map [96-127]     01 00 01 01 01 00 01 01 03 00 00 00 03 00 00 00
03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00
Standby Map [128-159]    03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00
03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 03
Standby Map [160-191]    00 00 03 00 00 03 00 00 03 00 00 03 00 00 03 00
02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02
Standby Map [192-223]    03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03
03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03
Standby Map [224-255]    03 03 03 03 03 03 03 03 03 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02

L2 Connectedness [0-31]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [32-63] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [64-95] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [96-127] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [128-159] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [160-191] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1

```



```

L2 Connectedness [192-223]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
L2 Connectedness [224-255]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1

Current Map Timestamp Wed Jun  1 12:17:57 2016 (2m:29s ago); gen_num=1
Reason=Node Up Trigger=Normal Bmap
Bucket Map Rcvd Timestamp Wed Jun  1 12:17:56 2016 (2m:30s ago)
radio_bg 0, radio_a 1:
Bucket Index 175, list 0x101ed464:
    sta:80:86:f2:41:1e:f0

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable mode on managed devices.

show ap remote debug bucketmap-counters

```
show ap remote debug bucketmap-counters {ap-name <ap-name> | ip-addr <ip-addr>
| ip6-addr <ip6-addr>}
```

Description

This command shows bucket map counters. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows bucket map counters filtered by specified AP name.
ip-addr <ip-addr>	Shows bucket map counters filtered by specified IP address of an AP.

Example

Access the CLI and use the following command to bucket map counters filtered by the AP name test:

```
(host) [mynode] #show ap remote debug bucketmap-counters ap-name test

Bucketmap Counters
-----
Name                                     Value
----                                     -
Bucketmap Updates, trunc errors         0 0
AP Bucketmap Updates Without Initialization 0
AP Bucketmap Lookup Failed              0
AP Bucketmap Allocation Failed          0
On AP STA Lookup UAC Failed             0
UAC Up/Down Events                      4 0
UAC Changed in Bmaps                   0
Deauth dropped from non-UAC             0
Deauths : New Bmap, Node Down not L2, node down no UAC 0, 0, 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable mode on managed devices.

show ap remote debug client-mgmt-counters

```
show ap remote debug client-mgmt-counters {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

Shows the number of each type of message from the clients of an AP. This information can be used to troubleshoot problems on an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
show ap remote debug client-mgmt-counters	Use this command to display message counters.
ap-name <ap-name>	To show message counters by AP name.
bssid <bssid>	To show message counters by MAC address of AP.
ip-addr <ip-addr>	To show message counters by IP address of AP.
ip6-addr <ip6-addr>	To show message counters by IPv6 address of AP.

Example

The output of this command shows client management counters for the specified AP:

```
(host)[mynode] #show ap remote debug client-mgmt-counters ap-name ap120-3
Counters
-----
Name                               Value
----                               -
Validate Client                     512
AP Stats Update Message              557750
3087                                 6
Tunnel VLAN Membership               4493
Update STA Tunnel Request            229
Update STA Tunnel Response           229
ARM Update                           808921
ARM Propagate                        590567
ARM Neighbor Assigned                55396
STM SAP Down                          19
AP Message                           192
```

```

STA On Call Message      12164
STA Message              19750
STA SIP authenticate Message 10919
STA Deauthenticate      707
Stat Update V3          441447
Remote AP State         371330
AP Message Response     164
assoc-req               4358
assoc-resp              4358
reassoc-req             950
reassoc-resp            950
disassoc                452
deauth                  5117
sapcp                   351131

```

Starting from ArubaOS 8.7.0.0, new counters were introduced for **ASAP AP APP stats messages and record counters** . The output of the following command displays the new counters:

```

(host) [mynode] #show ap remote debug client-mgmt-counters ip-addr 10.1.3.1
Counters
-----
Name
Value
----
-
SAPD SOS User Table flushed          3
...
WPA3-SAE assoc resp TX exception      0
Zone by src ip: zone 0 set, update, update_unchanged, clear, clear_err 1 0
0 0 0
Zone by src ip: zone 1 set, update, update_unchanged, clear, clear_err 0 0
0 0 0
Zone by src ip: zone 2 set, update, update_unchanged, clear, clear_err 0 0
0 0 0
Zone by src ip: zone 3 set, update, update_unchanged, clear, clear_err 0 0
0 0 0
Zone by src ip: zone 4 set, update, update_unchanged, clear, clear_err 0 0
0 0 0
Find zone by src ip: found, not found 0 0
ASAP AP APP stats messages total, null sap, empty, error 0,
0, 0, 0
AMON AP APP stats records queued, sent 0, 0

DPH TX txnid                          0
DPH TX total                          23

```

The output of this command includes the following information:

Parameter	Description
Validate Client	Number of times a client was validated.
AP Stats Update Message	Number of times an AP updated its statistics with the managed device.

Parameter	Description
ARM Update	Number of times an AP has changed its ARM settings.
STA On Call Message	Number of counters indicating that a station has an active phone call.
STA SIP authenticate Message	Number of messages indicating that a telephone has completed SIP registration and authentication.
STA Deauthenticate	Number of times a station sent a message to an AP to deauthenticate a client.
assoc-req	Number of 802.11 association request management frames from the controller.
assoc-resp	Number of 802.11 association responses to the controller.
reassoc-req	Number of 802.11 reassociation requests to the controller.
reassoc-resp	Number of 802.11 reassociation responses from the controller.
disassoc	Number of 802.11 disassociation messages to the controller.
deauth	Number of 802.11 deauthorization messages from the controller.

Command History

Release	Modification
ArubaOS 8.7.0.0	The following ASAP AP APP stats messages and record counters were introduced: <ul style="list-style-type: none"> ■ total ■ null sap ■ empty ■ error ■ queued ■ sent
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug flash-config

```
show ap remote debug flash-config {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>} acls | vap <vap> | vaps
```

Description

Show the remote AP configuration stored in flash memory.

Parameter	Description
ap-name <ap-name>	Shows debugging data for an AP with a specific name.
bssid <bssid>	Shows data for a specific BSSID on an AP. The BSSID is usually the MAC address of the AP.
ip-addr <ip-addr>	Shows data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IP6 address by entering its IP6 address in dotted-decimal format.
acls	Displays ACLs of offline virtual APs.
vap <vap>	Displays the configuration of a specific offline virtual AP by entering the name of a virtual AP.
vaps	Displays the current number of offline virtual APs.

Example

The output of this command can be used to debug problems with a remote AP. The command below shows statistics for an AP with the IP address 192.0.2.64.

```
(host) [mynode] #show ap remote debug flash-config ip-addr 192.0.2.64
acls
Offline ACLs
-----
Item                Value
----                -
Native VLAN        1
DHCP VLAN          N/A
DHCP ADDR          192.168.11.1
DHCP POOL NETMASK  255.255.255.0
DHCP POOL START    192.168.11.2
DHCP POOL END      192.168.11.254
DHCP DNS SERVER    0.0.0.0
DHCP ROUTER        192.168.11.1
DHCP DNS DOMAIN    mycompany
```



```

DHCP LEASE          0
Session ACL        N/A
Session ACL Name   N/A
Session ACL Count  N/A
Session Aces       N/A
ACL 1              1
ACL 1 Name         logon
ACL 1 Count        21
Aces 1             16 1 4294
...

```

The output of this command includes the following information:

Parameter	Description
Native VLAN	VLAN ID of the native VLAN.
DHCP VLAN	VLAN ID of Remote AP DHCP server used when the controller is unreachable.
DHCP ADDR	IP Address used as DHCP Server Identifier.
DHCP POOL NETMASK	Netmask of the DHCP server pool.
DHCP POOL START	IP Address used as the start of a range of addresses for a DHCP pool.
DHCP POOL END	IP Address used as the end of a range of addresses for a DHCP pool.
DHCP DNS SERVER	IP Address for the DHCP DNS server.
DHCP ROUTER	IP Address for the DHCP default router.
DHCP DNS DOMAIN	Domain name for the DHCP DNS server.
DHCP LEASE	Length of DHCP DNS leases in days. If this parameter displays a zero (0), the DHCP lease has no defined end.
Session ACL	Name of the ACL applied to the user session.
Session ACL name	Name of the ACL applied to the user session.
Session ACL count	Number of rules in the applied to the user session.
Session Aces	A list of the individual rules in the session ACL.
ACL 1	This parameter shows the position of an individual ACL.
ACL1 Name	Name of the ACL in the first position.
ACL1 Count	Number of rules in the specified ACL.

Parameter	Description
ACL1 Aces	A list of the individual rules in the specified ACL.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug-mcast-forwarder

```
show ap remote debug-mcast-forwarder {ap-name <ap-name> | ip-addr <ip-addr>
```

Description

This command displays the Mcast forwarder status for the selected AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows debugging information for a specific AP.
ip-addr <ip-addr>	Shows debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Example

Use this command to display the mcast forwarder status for an AP:

```
(host) [mynode] #show ap remote debug-mcast-forwarder ip-addr
191.191.191.323
Status (0): OFF, VLANs: 1
Mcast Aggregation Forwarder election status:
-----
VLAN  Forwarder  TX  RX
----  -
1     itself     0   0
Forwarder:mcast packets forwarder on the VLAN
TX:output announcement number for forwarder election on the VLAN
RX:input announcement number for forwarder election on the VLAN
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug mgmt-frames

```
show ap remote debug mgmt-frames {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>} [client-mac <client-mac>] [count <count>]
```

Description

This command shows traced 802.11 management frames for a remote AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Show debugging information for a specific AP.
ip-addr <ip-addr>	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.
client-mac <client-mac>	Show the AP associations for a specific MAC address by entering the MAC address of the client.
count <count>	Limit the amount of information displayed by specifying the number of frames to appear in the output of this command. Range: 1-128

Example

Use this command to debug 802.1 authentication on a remote AP. The example below shows that a client successfully associated with the remote AP, then was later deauthenticated.

```
(host) [mynode] #show ap remote debug mgmt-frames ap-name AP32
```

The output of this command includes the following information:

Parameter	Description
Timestamp	The time the management frame was sent.
stype	One of the following 802.11 frame types: auth: Authorization frame

Parameter	Description
	death: Deauthorization frame assoc-resp: Association response assoc-req: Association request
SA	Source MAC address.
DA	Destination MAC address.
BSS	BSSID of the AP.
signal	Signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Misc	Additional information describing the client's action. In the case of deauthentication, a reason associated with the event will be displayed in this column.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug neighbor-cache

```
show ap remote debug neighbor-cache {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command displays the per-ESSID neighbor cache of AP.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the wired port bounce configuration for the specified AP name.
ip-addr <ip-addr>	Shows the wired port bounce configuration for the specified IPv4 address.
ip6-addr <ip6-addr>	Shows the wired port bounce configuration for the specified IPv6 address.

Example

The following example displays the cached neighbors of a Wi-Fi 6E AP.

```
(host) [mynode] #show ap remote debug neighbor-cache ap-name hhm-635

Cached neighbors for 8@hhm-635-psk
-----
BSSID           Band  Channel  Operating Class  Signal  opmode  Flags
-----
cc:88:c7:41:64:60 6GHz  37       131              150     6       hWU

Flags: h = 802.11h support; W = WMM support; U = WMM UAPSD
       k = 802.11k support; R = 802.11r support
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the Band parameter.
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug nodelist history

```
show ap remote debug nodelist history {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows the cluster node history for a remote AP. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Show debugging information for a specific AP.
ip-addr <ip-addr>	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug nodelist history ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug redun-state history

```
show ap remote debug redun-state history {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows the cluster node history for a remote AP. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Show debugging information for a specific AP.
ip-addr <ip-addr>	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug redun-state history ap-name ap-205
Redun Event History
-----
PID and Time          Error          Event          Information
-----
[ 1717]1969-12-31 16:01:01  DISP INIT      INIT
TUNNEL_CONDUCTOR
[ 1717]1969-12-31 16:01:23  SEND ADD_CNODE_TUN  10.65.42.196
br0
[ 1717]1969-12-31 16:01:24  RECV PPP_UP      10.65.42.196
tun0
[ 1717]1969-12-31 16:01:24  DISP TUNNEL_UP    TUNNEL_CONDUCTOR
TUNNEL_LMS
[ 1717]2021-01-28 22:59:52  DISP CONFIG_NO_CHANGE  TUNNEL_LMS
UP
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sapd

```
show ap remote debug sapd cluster-nodestate
  ap-name
  ip-addr
  ip6-addr
```

Description

This command displays the state of cluster node in the SAPD process.

Parameter	Description
ap-name	Shows state of cluster node for specified AP name.
ip-addr	Shows state of cluster node for specified IP address.
ip6-addr	Shows state of cluster node for specified IPv6 address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Config mode in managed devices.

show ap remote debug stale_sta

```
show ap remote debug stale_sta {ap-name <ap-name> | bssid <bssid>| ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows information for debugging an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
show ap remote debug stale_sta	Shows stale station entries stored on the AP.
ap-name <ap-name>	Shows stale stations based on the AP name filter.
bssid <bssid>	Shows stale stations based on the AP MAC address filter.
ip-addr <ip-addr>	Shows stale stations based on the IP address filter of the AP.
ip6-addr <ip6-addr>	Shows stale stations based on the IPv6 address filter of the AP.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stale_sta ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The ip6-addr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sta-msg-sta-down-entries

```
show ap remote debug sta-msg-sta-down-entries {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows STA message for STA Down list. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows STA message for STA Down list of the specified AP.
ip-addr <ip-addr>	Shows STA message for Down list of the specified IP address.
ip6-addr <ip6-addr>	Shows STA message for Down list of the specified IPv6 address.

Example

The execution of the following command displays the STA Down list:

```
(host) [mynode] #show ap remote debug sta-msg-sta-down-entries ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The ip6-addr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sta-msg-stats

```
show ap remote debug sta-msg-stats {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows statistics of messages between AP and AC relating to STA associations on the AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows statistics of messages between AP and AC relating to STA associations for specified AP name.
ip-addr <ip-addr>	Shows statistics of messages between AP and AC relating to STA associations for specified IP address.
ip6-addr <ip6-addr>	Shows statistics of messages between AP and AC relating to STA associations for specified IPv6 address.

Example

The following example shows an example for executing this command:

```
(host) [mynode] #show ap remote debug sta-msg-stats ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The ip6-addr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug stm cluster-nodestate

```
show ap remote debug stm cluster-nodestate {ap-name <ap-name> | ip-addr <ip-addr>
| ip6-addr <ip6-addr>}
```

Description

This command shows the cluster node state in AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the cluster node state for specified AP name.
ip-addr <ip-addr>	Shows the cluster node state for specified IP address.
ip6-addr <ip6-addr>	Shows the cluster node state for specified IPv6 address.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stm cluster-nodestate ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The ip6-addr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug stm trace-files

```
show ap remote debug stm trace-files {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows STM trace files for an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the STM trace files for specified AP name.
ip-addr <ip-addr>	Shows the STM trace files for specified IP address.
ip6-addr <ip6-addr>	Shows the STM trace files for specified IPv6 address.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stm trace-files ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug uac-list

```
show ap remote debug uac-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows user anchor controller (UAC) list in AP datapath. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the UAC list in AP datapath for the specified AP name.
ip-addr <ip-addr>	Shows the UAC list in AP datapath for the specified IP address.
ip6-addr <ip6-addr>	Shows the UAC list in AP datapath for the specified IPv6 address.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug uac-list ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug web-server-config

```
show ap remote debug web-server-config {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command displays the web server profile configurations on the AP.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the web server profile configuration for the specified AP name.
ip-addr <ip-addr>	Shows the web server profile configuration for the specified IPv4 address.
ip6-addr <ip6-addr>	Shows the web server profile configuration for the specified IPv6 address.

Example

The following example displays the web server profile fields configured on APs:

```
(host) [mynode] (config) #show ap remote debug web-server-config ip-addr 10.65.39.213

Web Server Configuration
-----
Cipher  SSL      Cert
-----  ---      ----
high    tlsv1.2  default
```

The output of this command includes the following parameters:

Parameter	Description
Cipher	The cipher suite strength displaying one of the following values: <ul style="list-style-type: none">■ high■ medium■ low high

Parameter	Description
SSL	The SSL/TLS protocol type displaying one of the following values: <ul style="list-style-type: none"> ■ tlsv1 ■ tlsv1.1 ■ tlsv1.2 tlsv1.2
Cert	The server certificate for captive portal.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug wired-port-down-state

```
show ap remote debug wired-port-down-state {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command displays the wired port bounce configurations that are forwarded from the controller and AP's wired port status.

The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the wired port bounce configuration for the specified AP name.
ip-addr <ip-addr>	Shows the wired port bounce configuration for the specified IPv4 address.
ip6-addr <ip6-addr>	Shows the wired port bounce configuration for the specified IPv6 address.

Example

The following example displays AP's wired port status and the wired port bounce configurations that are forwarded from the controller:

```
(host) [mynode] #show ap remote debug wired-port-down-state ap-name ap-test

The configurations pushed from the controller
-----
The port bounce time by disable POE: 30
The port bounce time by shutdown ethernet link: 60
AP's wired port is in down time, the port status as below
-----
All wired ports' status
-----
Wired port Ethernet link status Whether Support PSE PSE status
-----
eth0          up                no
eth1          down              no
eth2          down              no
eth3          up                yes                enable
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote essid

```
show ap remote essid {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

Shows an ESSID summary for the Managed Device, including the numbers of APs and clients connected to a managed device. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the ESSID summary for the specified AP name.
bssid <bssid>	Shows the ESSID summary for the specified MAC address.
ip-addr <ip-addr>	Shows the ESSID summary for the specified IP address.
ip6-addr <ip6-addr>	Shows the ESSID summary for the specified IPv6 address.

Example

The following is an example for executing the `show ap remote essid` command:

```
(host) [mynode] #show ap remote essid ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote wmm-flow

```
show ap remote wmm-flow {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows the Wireless Multimedia (WMM) flows that are active on an AP connected to a Managed Device. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the WMM flows that are active for a specified AP name.
bssid <bssid>	Shows the WMM flows that are active for a specified MAC address.
ip-addr <ip-addr>	Shows the WMM flows that are active for a specified IP address.
ip6-addr <ip6-addr>	Shows the WMM flows that are active for a specified IPv6 address.

Example

The following is an example for executing the `show ap remote wmm-flow` command:

```
(host) #show ap remote wmm-flow ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ip6-addr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap sapd-debug log

```
show ap sapd-debug log {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} | <page>
```

Description

This command displays the SAPD debug log for an AP. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Shows the SAPD debug log for the specified AP name.
ip-addr <ip-addr>	Shows the SAPD debug log for the specified IP address.
ip6-addr <ip6-addr>	Shows the SAPD debug log for the specified IPv6 address.
<page>	Displays the specified page of the SAPD debug log information.

Example

The following is an example for executing the `show ap sapd-debug log` command:

```
(host) #show ap sapd-debug log ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap snmp

```
show ap snmp
  wlsxSwitchStationMgmtTable
  wlsxSwitchStationStatsTable
  wlsxWlanAPBssidTable
  wlsxWlanAPTable
  wlsxWlanESSIDTable
  wlsxWlanRadioTable
```

Description

This command displays the AP-related SNMP tables.

Parameter	Description
wlsxSwitchStationMgmtTable	Display user tree.
wlsxSwitchStationStatsTable	Display user statistics tree.
wlsxWlanAPBssidTable	Display BSSID SNMP tree.
wlsxWlanAPTable	Display SNMP tree.
wlsxWlanESSIDTable	Displays ESSID SNMP tree.
wlsxWlanRadioTable	Display radio table SNMP tree.

Example

The following command displays BSSID SNMP tree (For versions prior to ArubaOS 8.9.0.0).

```
(host)[mynode] #show ap snmp wlsxWlanAPBssidTable

SNMP - AP BSSID Table
-----
AP MAC           Radio  BSSID           Phy Type  Status  Channel
-----
00:24:6c:c3:d6:82  1     00:24:6c:bd:68:30  1         1       149
00:24:6c:c3:d6:82  2     00:24:6c:bd:68:20  2         1       11

Num BSSIDs:2
```

The following command displays BSSID SNMP tree for a Wi-Fi 6E AP(For ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #show ap snmp wlsxWlanAPBssidTable

SNMP - AP BSSID Table
-----
AP MAC           Radio  BSSID           Phy Type  Status  Channel
-----
84:d4:7e:c6:61:74  1     84:d4:7e:e6:17:50  1         1
5GHz/52E/80MHz/VHT
cc:88:c7:cc:16:46  3     cc:88:c7:41:64:60  4         1
6GHz/37S/160MHz/HE

Num BSSIDs:2
```

Related Commands

Command	Description
snmp-server	This command configures SNMP parameters.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include 2.4GHz , 5GHz , and 6GHz values for Channel parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on managed devices.

show ap spectrum ap-list

```
show ap spectrum ap-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [channel <channel> | essid <ssid> | freq-band {2.4ghz | 5ghz} | limit <limit> | or | page <page> | sort <sort> | start <start>]
```

Description

This command shows spectrum data seen by an access point that has been converted to a spectrum monitor.

The Spectrum Analysis feature provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify 802.11 devices on the network. Use this command to display and sort APs seen by a specific spectrum monitor.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor for which you want to view spectrum information.
channel <channel>	View spectrum information for a specific radio channel.
ssid <ssid>	View spectrum information for a specific ESSID.
freq-band {2.4ghz 5ghz}	View information for a specific radio type, either 2.4 GHz or 5 GHz.
limit <limit>	Limit the displayed output to the specified number of entries
or	Use this parameter to display information that meets either of two criteria, such as a specified ESSID or channel.
page <page>	Enter a number from 10–100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
sort <sort>	Sort the output by the specified data column.
start <start>	Start displaying the output at specific spectrum index value.

Example

The output of this example shows spectrum data seen by spectrum monitor ap123. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host) [mynode]# show ap spectrum ap-list ap-name ap123

Spectrum AP Table
-----
bssid          essid          spectrum-id  chan  phy-type      signal
(dBm)
-----
-----
00:0b:86:cd:22:d0  ECSD Wireless  2           161  80211a        62
00:0b:86:cb:cf:30  ECSD Wireless  3           157  80211a        68
00:0b:86:f6:f6:a0  osuwireless    3           1    80211b/g      48
00:0b:86:f6:f6:a1  osuvoice       4           1    80211b/g      47
00:0b:86:f6:f6:a2  osuguest       5           1    80211b/g      45

avg-rssi (dB)  curr-rssi (dB)  ibss  add-time          last-seen
-----
29             31             no    2010-05-16 17:41:36  2010-05-18 13:39:38
24             25             no    2010-05-16 17:41:36  2010-05-18 14:19:03
37             38             no    2010-05-16 17:41:36  2010-05-18 15:06:02
38             38             no    2010-05-16 17:41:36  2010-05-18 15:04:23
37             40             no    2010-05-16 17:41:36  2010-05-18 15:07:32
```

The output of this command includes the following information:

Column	Description
bssid	Basic Service Set Identifier for an AP. This is usually the MAC address of the AP.
ssid	Extended Service Set Identifier that names a wireless network.
spectrum-id	Identifier assigned to the device by the spectrum monitor.
chan	Radio channel used by the BSSID.
freq-band	Radio phy type. Possible types include: <ul style="list-style-type: none"> 2.4 GHz 5 GHz
signal (dBm)	Strength of the signal received by the device, in dBm.
avg-rssi	The average signal-to-noise ratio seen by the AP.
curr-rssi	Most recent signal-to-noise ratio seen by the AP.

Column	Description
ibss	Shows if ad hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad hoc BSS (an ibss bit in an 802.11 frame).
add-time	Time when the AP was first detected by the spectrum monitor.
last-seen	Time when the AP was last seen by the spectrum monitor.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum channel-metrics

```
show ap spectrum channel-metrics {ap-name <ap-name>|ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz}]
```

Description

This command shows channel quality, availability, and utilization metrics as seen by a spectrum monitor.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor.
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.
freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)	View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz. NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.

This chart displays channel utilization data, showing the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 adjacent channel interference (ACI).

ACI refers to the interference on a channel created by a transmitter operating in an adjacent channel. A transmitter on a nonadjacent or partially overlapping channel may also cause interference, depending on the transmit power of the interfering transmitter and/or the distance between the devices. In general, ACI may be caused by a Wi-Fi transmitter or a non-Wi-Fi interferer. However, whenever the term ACI appears in Spectrum Analysis graphs, it refers to the ACI caused by Wi-Fi transmitters. The channel utilization option in the Channel Metrics Chart shows the percentage of the channel utilization due to both ACI and non-Wi-Fi interfering devices. Unlike the ACI shown in the [show ap spectrum interference-power](#) output, the ACI shown in this graph indicates the percentage of channel time that is occupied by ACI or unavailable for Wi-Fi communication due to ACI.



The Channel Metrics table can also show channel availability, the percentage of each channel that is available for use, or display the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. In the spectrum analysis feature, channel quality is a relative measure that indicates the ability of the channel to support reliable Wi-Fi communication. Channel quality, which is represented as a percentage in this chart, is a weighted metric derived from key

parameters that can affect the communication quality of a wireless channel, including noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of retries. Note that channel quality is not directly related to Wi-Fi channel utilization, as a higher quality channel may or may not be highly utilized.



A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non- Wi-Fi data.

Example

The output of this example shows part of the channel metrics table for channels seen by the spectrum monitor ap123:

```
(host) [mynode] #show ap spectrum channel-metrics ap-name ap123 freq-band
2.4ghz

Channel Metrics Table
-----
Channel  Quality(%)  Availability(%)  Utilization(%)  WiFi Util(%)
Interference Util(%)
-----
1         97             57              43              40              3
2         80             58              42              22              20
3         63             58              42              5               37
4         71             57              43              16              27
5         88             54              46              36              10
6         98             51              49              47              2
7         88             54              46              35              11
8         69             56              44              14              30
9         60             57              43              3               40
10        30             29              71              1               70
11        0              0               100             0               100
12        25             50              50              0               50
13        50             99              1               0               1
14        99             99              1               0               1
1+/5-    63             54              46              36              10
2+/6-    63             51              49              47              2
3+/7-    63             51              49              47              2
4+/8-    69             51              49              47              2
5+/9-    60             51              49              47              2
6+/10-   30             29              71              1               70
7+/11-   0              0               100             0               100
```

The output of this command includes the following information:

Column	Description
channel	An 802.11a or 802.11g radio channel.

Column	Description
Quality(%)	Current relative quality of selected channels in the 802.11a or 802.11g radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non- Wi-Fi devices on that channel.
Availability(%)	The percentage of the channel currently available for use.
Utilization(%)	The percentage of the channel being used.
WiFi Util(%)	The percentage of the channel currently being used by Wi-Fi devices.
Interference Util(%)	The percentage of the channel currently being used by non-Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profile mode spectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum channel-summary

```
show ap spectrum channel-summary {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz}]
```

Description

This command displays a summary of the 802.11a or 802.11g channels seen by a spectrum monitor.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor for which you want to view spectrum information.
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.
freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)	View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz. NOTE: The 6ghz sub-

Parameter	Description
	parameter is applicable to Wi-Fi 6E APs only.

The output of the table can display data aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference, and the Signal-to-Noise-and-Interference Ratio (SNIR).

SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.



A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non- Wi-Fi data.

Example

The output of the example below shows information for 802.11a radio channels seen by the spectrum monitor **ap999**.

```
(host) [mynode] #show ap spectrum channel-summary ap-name ap999 freq-band
5ghz

Channel Summary Table
-----
Channel   KnownAPs  UnknownAPs  Util(%)  MaxAPSignal (dBm)  MaxInterference
(dBm)    SNIR (dB)
-----
--  -----
149      69         0           5        -39              -69
 30
153      20         0          100       -42              -60
 18
157      56         0           6        -53              -59
  6
161      54         0           4        -43              -71
 28
165      32         0           3        -27              -70
 43
149+     69         0          100       -39              -60
 21
157+     20         0           6        -43              -59
 16
```

The output of this command includes the following information:

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference (dBm)	Signal strength of the non- Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Related Commands

Command	Description
<u>ap spectrum local-override</u>	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
<u>rf dot11a-radio-profilemodespectrum-mode</u>	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum client-list

```
show ap spectrum client-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [ap-bssid <ap-bssid> | channel <channel> | essid <essid> | freq-band {2.4ghz | 5ghz} | limit <limit> | mac <mac> | or | page <page> | sort <sort> | start <start>]
```

Description

This command shows details for clients seen by a specified spectrum monitor.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor for which you want to view spectrum information.
ap-bssid <ap-bssid>	View information for a client with a specific BSSID.
band <band>	View information for specific radio band. The possible values are 2.4ghz, 5ghz, or 6ghz.
channel <channel>	view information for clients on a specific radio channel.
essid <essid>	View information for clients using a specific ESSID.
mac <mac>	View information for a client with a specific MAC address.
or	Use this parameter to display information that meets either or two criteria, such as a specified ESSID or channel.
page <page>	Enter a number from 10–100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
sort <sort>	Sort the output by the specified data column.
start <start>	Start displaying the output at specific spectrum index value.

Example

The following example shows that the spectrum monitor **ap999** sees eight different clients on channel 149. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host) [mynode] #show ap spectrum client-list ap-name ap999 channel 149

Spectrum Client Table
-----
mac          bssid          essid          spectrum-id
channel phy-type
---
-
00:14:a4:d1:34:63 00:24:6c:80:48:79 ethersphere-wpa2 14          149
80211a
00:19:7d:3a:96:d9 00:24:6c:80:7b:c9 ethersphere-wpa2 198         149
80211a
00:16:cf:af:3e:e1 00:24:6c:80:48:79 ethersphere-wpa2 80          149
80211a
00:1c:26:5b:a7:ac 00:24:6c:81:8b:19 ethersphere-wpa2 125         149
80211a
00:21:6b:c6:b2:12 00:24:6c:80:48:79 ethersphere-wpa2 118         149
80211a-HT-40
00:21:6a:9c:0e:36 00:24:6c:81:8b:19 ethersphere-wpa2 121         149
80211a
00:21:6a:51:e4:30 00:1a:1e:87:c1:91 ethersphere-wpa2 164         149
80211a-HT-40
00:24:d6:65:a9:e6 00:24:6c:80:48:7a ethersphere-voip 222         149
80211a-HT-40

signal (dBm)    add-time          last-seen
-----
-71             2010-05-17 09:53:47 2010-05-17 12:36:54
-66             2010-05-17 12:01:01 2010-05-17 12:36:42
-74             2010-05-17 09:54:59 2010-05-17 12:35:55
-79             2010-05-17 10:23:29 2010-05-17 12:37:28
-66             2010-05-17 10:17:05 2010-05-17 12:31:58
-72             2010-05-17 10:20:05 2010-05-17 12:37:30
-63             2010-05-17 11:07:21 2010-05-17 12:29:01
-69             2010-05-17 12:37:25 2010-05-17 12:37:25

start:0
Length:8
Total:8
```

The output of this command includes the following information:

Column	Description
mac	MAC address of the client.

Column	Description
bssid	Basic Service Set Identifier for a client. This is usually the device's MAC address.
essid	Extended service set identifier that names a wireless network.
spectrum-id	Identifier assigned to the client by the spectrum monitor.
chan	Radio channel used by the BSSID.
phy-type (For versions prior to ArubaOS 8.9.0.0)	Radio phy type. Possible types include: <ul style="list-style-type: none"> ▪ 802.11a ▪ 802.11a-HT-40 ▪ 802.11b/g ▪ 802.11b/g-HT-20
band (For ArubaOS 8.9.0.0 or later versions)	Radio band type. Possible types include: <ul style="list-style-type: none"> ▪ 2.4ghz ▪ 5ghz ▪ 6ghz (For Wi-Fi 6E APs)
signal (dBm)	Client signal strength, in dBm.
add-time	Time when the client was first detected by the spectrum monitor.

Column	Description
<code>last-seen</code>	Time when the spectrum monitor last detected that the client was active.

Related Commands

Command	Description
<code>ap spectrum local-override</code>	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
<code>rf dot11a-radio-profilemodespectrum-mode</code>	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
<code>rf dot11g-radio-profilemodespectrum-mode</code>	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The <code>band <band></code> parameter was introduced. ■ Replaced <code>phy-type</code> with <code>band</code> in the command output parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug

```
show ap spectrum debug {channel-info | channel-quality | classify |classify-device  
| classify-fft | device-details | device-info | devices-seen} {ap-name <ap-name> |  
ip-addr <ip-addr> | ip6-addr <ip6-addr>} freq-band {2.4ghz | 5ghz} radio {0 | 1 |  
2} [<count>]
```

Description

This command saves spectrum analysis channel information to a file on the spectrum monitor. Use this command under the supervision of your Aruba technical support representative to troubleshoot spectrum analysis issues or errors. If a dump-server is defined in the AP system profile of the AP, the file created by this command will be sent from the AP to the dump-server using TFTP.

Parameter	Description
channel-info	Save channel information for later analysis.
channel-quality	Save channel quality information for later analysis
classify	Save information on classification for later analysis.
classify-device	Save information on classification-related debugging with device-type for later analysis.
classify-fft	Save information on classification and FFT data for later analysis.
device-details	Save device details for later analysis.
device-info	Save device information for later analysis.
devices-seen	Save information on devices seen by the spectrum monitor.
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor for which you want to view spectrum information.
freq-band {2.4ghz 5ghz}	Save information for a specific radio type, either 2.4 GHz or 5 GHz .
radio {0 1 2}	Save information for a specific radio type, either 0, 1, or 2 . Radio 0, 1 or 2 is supported only on AP-555 access points.
<count>	Specify the number of samples to save.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug channel-info ap-name ap-205 freq-band 2.4ghz 22
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.6.0.0	The parameter <code>radio {0 1 2}</code> was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug fft

```
show ap spectrum debug fft {ap-name <ap-name> | ip-addr <ip-addr>} | ip-6 addr <ip6-addr>} freq-band {2.4ghz | 5ghz} [avg | duty-cycle | fft-to-controller | max | normalized | raw | raw-normalized] [<count>]
```

Description

This command helps you save Fast Fourier Transform (FFT) power data to a file on the spectrum monitor. Use this command under the guidance of your Aruba technical support representative to troubleshoot FFT power issues.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor.
freq-band {2.4ghz 5ghz}	Save information for a specific radio type, either 2.4 GHz or 5 GHz .
avg	Save FFT average information.
duty-cycle	Save FFT duty-cycle data.
fft-to-controller	Save the FFT max, average, and duty-cycle data.
max	Save the maximum FFT power measured for all samples taken over the last second.
normalized	Save normalized FFT information.
raw	Save the raw FFT information received from a driver.
raw-normalized	Save FFT information received from a driver and its normalized FFT.
count	Save a specific number of samples.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug fft ap-name ap-205 freq-band 5ghz avg 20
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profile mode spectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug monitors

show ap spectrum debug monitors

Description

Shows a detailed description of all spectrum monitors on the controller. Use this command under the guidance of an Aruba technical support representative to troubleshoot spectrum analysis errors.

Example

The output of this command shows a list of available spectrum monitor or hybrid AP devices, a list of spectrum devices currently subscribed to a spectrum client, message counters for subscribed spectrum devices, and the subscription history:

```
(host) [mynode] #show ap spectrum debug monitors
List of Available Sensors
-----
AP name  Phy  Band
-----  -  -
ap999    G   2GHz
ap999    A   5GHz
Total: 2
List of Subscriptions
-----
AP name  Band          Client IP      Subscribe Time      HTTPD pid  Last
Data Sent  Send Failed
-----  -  -
ap123    2GHz          10.100.100.67  2010-05-18 03:49:44 PM  1711      1s
0
ap123    5GHz          10.100.100.67  2010-05-18 03:49:51 PM  1711      1s
0
Num Subscriptions: 2
Current Time: 2010-05-18 03:49:54 PM
Message Counters
-----
AP name  Band          FFT Data  FFT Duty Cycle  Device Info  Device Details
Devices Seen  Channel Info
-----  -  -
ap123    2GHz          4          4              1            194
1
ap123    5GHz          0          0              0            0
0
Subscription History
-----
Message          AP/Radio/Band          Client IP      HTTPD  Timestamp
Result
pid
```

```

-----
-----
Subscribe      "ap123"/1/2GHz      10.240.16.165  1701  2010-05-17
01:29:16 PM  Success
Re-subscribe   "ap123"/0/5GHz     10.240.16.165  1700  2010-05-17
01:29:16 PM  Success
Unsubscribe-All "ap123"/-/-        10.240.16.165  1701  2010-05-17
02:44:18 PM  Client Not found
Subscribe      "ap123"/1/2GHz     10.100.100.67  1716  2010-05-18
03:44:28 PM  Success

```

Related Commands

Command	Description
ap spectrum local-override	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Set an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profile mode spectrum-mode	Set an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output displays the details of Radio 0, 1 and 2 for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug status

```
show ap spectrum debug status {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz}]
```

Description

This command shows detailed status and statistics for a spectrum monitor or hybrid AP. Use the command under the guidance of an Aruba technical support representative to troubleshoot spectrum analysis errors.

Parameter	Description
ap-name <ap-name>	Name of the spectrum device for which you want to view status information.
ip-addr <ip-addr>	IP address of the spectrum device for which you want to view status information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum device for which you want to view status information.
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.
freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)	View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz. NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug status ap-name ap-205 freq-band 5ghz
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.

Command	Description
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Set an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-duty-cycle

```
show ap spectrum device-duty-cycle {ap-name <ap-name>| ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz}] radio {0 | 1 | 2}
```

Description

This command shows the current duty cycle for devices on all channels being monitored by the spectrum monitor or hybrid AP radio.

Parameter	Description
ap-name <ap-name>	Name of the spectrum device for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum device for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum device for which you want to view spectrum information.
freq-band 2.4ghz 5ghz	View information for a specific radio type, either 2.4 GHz or 5 GHz.
radio {0 1 2}	View information for a specific radio type, either 0, 1 or 2. Radio 0, 1 or 2 is supported only on AP-555 access points.

The FFT Duty Cycle table in the output of this command shows the duty cycle for each radio channel. The duty cycle is the percentage of time each device type operates or transmits on that channel. For additional details about non- Wi-Fi device types shown in this table, see [Non-Wi-Fi Interferers on page 2433](#).

Examples

The output of this command shows that video devices sent a signal on channels 153 and 157 during 99% of the last sample interval:

```
Device Duty Cycle Table (in %)
-----
Device Type          149  153  157  161  165  149+  157+
-----
Generic Interferer   0    0    0    0    0    0    0
WIFI                  5    0    5   12    8    0   12
Microwave             0    0    0    0    0    0    0
Bluetooth             0    0    0    0    0    0    0
Generic Fixed Freq    0    0    0    0    0    0    0
Cordless Phone FF    0    0    0    0    0    0    0
Video                 0   99   99    0    0    0    0
```



```

Audio          0  0  0  0  0  0  0
Generic Freq Hopper 0  0  0  0  0  0  0
Cordless Network FH 0  0  0  0  0  0  0
Xbox           0  0  0  0  0  0  0
Microwave Inverter 0  0  0  0  0  0  0
Cordless Base FH  5  5  5  5  5  0  0
Total: 7

```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.6.0.0	The parameter <code>radio {0 1 2}</code> was introduced for AP-555 access points.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-history

```
show ap spectrum device-history {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz}] [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base | cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-inverter | video | xbox}]
```

Description

This command shows the history of the last 256 non-Wi-Fi devices. Use this command to view channel, signal, and duty-cycle information as well as add or delete times for the last 256 devices seen by a spectrum monitor or hybrid AP.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Parameter	Description
<p>freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)</p>	<p>View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz.</p> <p>NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.</p>
<p>type</p>	<p>Show information for one type of device only by specifying a non- Wi-Fi device.</p>
<p>audio</p>	<p>View information for audio devices seen by the spectrum device.</p>
<p>bluetooth</p>	<p>View information for Bluetooth devices seen by the spectrum device.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum devices.</p>
<p>cordless-ff-phone</p>	<p>View information for frequency-hopping cordless phones seen by the spectrum device.</p>

Parameter	Description
cordless-fh-base	View information for frequency-hopping cordless phone bases seen by the spectrum device.
cordless-fh-network	View information for frequency-hopping cordless network devices seen by the spectrum device.
generic-ff	View information for generic fixed-frequency devices seen by the spectrum device.
generic-fh	View information for generic frequency-hopping devices seen by the spectrum device.
generic-interferer	Show only generic interfering devices.
microwave	View information for microwave-emitting devices seen by the spectrum device. NOTE: This option is available only for 2.4 GHz

Parameter	Description
	spectrum devices.
microwave-inverter	View information for inverter microwave devices seen by the spectrum device. NOTE: This option is available only for 2.4 GHz spectrum devices.
video	View information for video devices seen by the spectrum device.
xbox	View information for Xbox devices seen by the spectrum device. NOTE: This option is available only for 2.4 GHz spectrum devices.

Non-Wi-Fi Interferers

The following table describes each type of non-Wi-Fi interferer detected by a spectrum monitor or hybrid AP. Note also that a hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Non-Wi-Fi Interferer Type	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a <i>Bluetooth</i> device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as <i>Fixed Frequency (Audio)</i> .
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as <i>Fixed Frequency (Cordless Phones)</i> .
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as <i>Fixed Frequency (Video)</i> . These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV, or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as <i>Fixed Frequency (Other)</i> . Note that the RF signatures of the fixed frequency audio, video, and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as <i>Frequency Hopper (Cordless Base)</i> .
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as <i>Frequency Hopper (Cordless Network)</i> . Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as <i>Frequency Hopper (Xbox)</i> .
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles, and cordless or hands-free devices that do not use one of the known cordless phone protocols.

Non-Wi-Fi Interferer Type	Description
Microwave	Common residential microwave ovens with a single magnetron are classified as a <i>Microwave</i> . These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as <i>Microwave (Inverter)</i> . Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare, or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a <i>Generic Interferer</i> . For example, a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum device-history ap-name ap-205 type audio
```

The output of this example shows details for fixed-frequency video devices seen by a spectrum monitor or hybrid AP radio:

```
host) [mynode] #show ap spectrum device-history ap-name ap123 freq-band 5ghz
type video

Non-Wifi Device History Table
-----
Type   ID   Cfreq(Khz)  Bandwidth(KHz)  Channels-affected  Signal-strength
Duty-cycle
-----
-----
Add-time           Delete-time
-----
Video 1   5745312    6000           149             76              99
2010-05-16 20:07:08  -
```

Video 2	5745312	6000	149	75	99
2010-05-16 20:07:39	2010-05-17 16:50:24				
Video 3	5745312	6000	149	74	99
2010-05-16 20:20:25	2010-05-16 20:20:36				
Video 4	5745312	6000	149	76	99
2010-05-16 20:32:44	2010-05-16 20:33:07				
Video 5	5742031	6000	149	79	99
2010-05-16 20:33:43	2010-05-16 20:33:53				
Video 6	5745312	6000	149	75	99
2010-05-16 20:34:08	2010-05-16 20:34:20				

The output of this command includes the following information:

Column	Description
Type	<p>Device type. This parameter can be any of the following:</p> <ul style="list-style-type: none"> ▪ audio FF (fixed frequency) ▪ bluetooth ▪ cordless base FH (frequency hopper) ▪ cordless phone FF (fixed frequency) ▪ cordless network FH (frequency hopper) ▪ generic FF (fixed frequency) ▪ generic FH (frequency hopper) ▪ generic interferer ▪ microwave ▪ microwave inverter ▪ video ▪ xbox <p>NOTE: For additional details about non- Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 2433.</p>
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device, in KHz.
Channels-affected	Radio channels affected by the wireless device, in KHz.
Signal-strength	Strength of the signal sent from the device, in dBm.

Column	Description
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts on the specified channel or frequency.
Add-time	Time at which the device was first detected.
Delete-time	Time at which the device was aged out.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The 6ghz sub-parameter was introduced for freq-band parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-list

```
show ap spectrum device-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz} [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base | cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-inverter | video | xbox}]]
```

Description

Shows a device summary table and channel information for non-Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip6-addr <ip-addr>	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
freq-band {2.4ghz 5ghz} 8.9.0.0 (For versions prior to ArubaOS	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Parameter	Description
<p>freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)</p>	<p>View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz.</p> <p>NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.</p>
<p>type</p>	<p>Show data for a specific device type only.</p>
<p>audio</p>	<p>Show only audio fixed frequency devices.</p>
<p>bluetooth</p>	<p>Show only Bluetooth devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum devices.</p>
<p>cordless-ff-phone</p>	<p>View information for frequency-hopping cordless phones seen by the spectrum device.</p>
<p>cordless-fh-base</p>	<p>View information for frequency-hopping cordless phone bases seen by the spectrum device.</p>

Parameter	Description
cordless-fh-network	View information for frequency-hopping cordless network devices seen by the spectrum device.
generic-ff	View information for generic fixed-frequency devices seen by the spectrum device.
generic-fh	View information for generic frequency-hopping devices seen by the spectrum device.
generic-interferer	Show only generic interfering devices.
microwave	<p>Show only microwave devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum devices.</p>
microwave-inverter	<p>Show only microwave inverter devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum</p>

Parameter	Description
	devices.
video	Show only video fixed frequency devices.
xbox	Show only Xbox frequency hopper devices. NOTE: This option is available only for 2.4 GHz spectrum devices.

Use the optional `type` parameter to display data for one specific device type only. For additional details about non-Wi-Fi device types shown in this table, see [Non-Wi-Fi Interferers on page 2433](#).



A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Example

The output of this example shows that the spectrum monitor **ap123** is able to see data for a single non-Wi-Fi device on its 802.11a radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) [mynode] #show ap spectrum device-list ap-name ap123 freq-band 5ghz
Non-Wifi Device List Table
-----
Type          ID  Cfreq   Bandwidth  Channels-affected  Signal-
strength
-----
-
Cordless Phone FH  3   5826093  80000      149 157 161 165    49
Duty-cycle   Add-time          Update-time
-----
5           2010-05-17 10:04:53  2010-05-17 10:04:55
Total: 1
Current Time: 2010-05-17 10:04:56
```

The output of this command includes the following information:

Column	Description
Type	<p>Device type. This parameter can be any of the following:</p> <ul style="list-style-type: none"> ▪ audio FF (fixed frequency) ▪ bluetooth ▪ cordless base FH (frequency hopper) ▪ cordless phone FF (fixed frequency) ▪ cordless network FH (frequency hopper) ▪ generic FF (fixed frequency) ▪ generic FH (frequency hopper) ▪ generic interferer ▪ microwave ▪ microwave inverter ▪ video ▪ Xbox <p>NOTE: For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 2433.</p>
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the status of the device was updated.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command	Description
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-log

```
show ap spectrum device-log {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz | 6ghz} [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base | cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-inverter | video | xbox}]
```

Description

This command shows a time log of add and delete events for non-Wi-Fi devices.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor for hybrid AP or which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip6-addr <ip6-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.
freq-band {2.4ghz 5ghz 6ghz} versions) (For ArubaOS 8.9.0.0 or later)	View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz.

Parameter	Description
	<p>NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.</p>
type	Show data for a specific device type only.
audio	Show only audio fixed frequency devices.
bluetooth	<p>Show only Bluetooth devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum device radios.</p>
cordless-ff-phone	View information for frequency-hopping cordless phones seen by the spectrum device.
cordless-fh-base	View information for frequency-hopping cordless phone bases seen by the spectrum device.

Parameter	Description
cordless-fh-network	View information for frequency-hopping cordless network devices seen by the spectrum device.
generic-ff	View information for generic fixed-frequency devices seen by the spectrum device.
generic-fh	View information for generic frequency-hopping devices seen by the spectrum device.
generic-interferer	Show only generic interfering devices.
microwave	<p>Show only microwave devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum device radios.</p>
microwave-inverter	<p>Show only microwave inverter devices.</p> <p>NOTE: This option is available only for 2.4 GHz spectrum</p>

Parameter	Description
	device radios.
video	Show only video fixed frequency devices.
xbox	Show only Xbox frequency hopper devices. NOTE: This option is available only for 2.4 GHz spectrum device radios.



A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Example

The output of this example shows that the spectrum monitor **ap123** logged data for four frequency-hopping cordless base devices seen by its 802.11g radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) [mynode] #show ap spectrum device-log ap-name ap123 freq-band 5ghz
type cordless-fh-base

Non-Wifi Device Log Table
-----
Device Type      ID  Added/Deleted  Signal Strength  Duty Cycle  Center
Freq
-----
-
Cordless Base FH 1  Added          78              5             5773281
Cordless Base FH 1  Deleted        78              5             5747343
Cordless Base FH 2  Added          78              5             5757656
Cordless Base FH 2  Deleted        78              5             5760469
Cordless Base FH 3  Added          80              5             5802813
Cordless Base FH 3  Deleted        80              5             5802813
Cordless Base FH 4  Added          80              5             5770781

Start Freq  End Freq  Channels Affected  Bandwidth
-----
```

```

5733281      5813281      153              80000
5707343      5787343      149 153 157 161 165 80000
5717656      5797656      153              80000
5720469      5800469      153 157 161 165 80000
5762813      5842813      161              80000
5762813      5842813      161              80000
5730781      5810781      153              80000

```

```

Total: 7
Current Time: 2012-09-25 12:04:54

```

The output of this command includes the following information:

Column	Description
Device Type	Type of non-Wi-Fi device detected by the spectrum monitor or hybrid AP
ID	The spectrum ID number assigned to that device. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Added/Deleted	The non-Wi-Fi Device Log table can show signal data for a device when that device was added or removed from the log table.
Signal Strength	Strength of the signal sent by the device.
Duty Cycle	Device duty cycle. This value represents the percent of time a signal is broadcast on a specific channel or frequency.
Center Freq	Center frequency of the signal sent by the device.
Start Freq	Lowest signal frequency sent by the device.
End Freq	Highest signal frequency sent by the device.
Channels affected	Radio channels affected by the device signal.
Bandwidth	Amount of signal bandwidth used by the device, in Kilohertz.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.

Command	Description
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-summary

```
show ap spectrum device-summary
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  freq-band {2.4 GHz | 5 GHz}
```

Description

This command shows the numbers of Wi-Fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor or hybrid AP. Use this command to show the types of devices that the spectrum device can detect on each channel it monitors. For additional details about non-Wi-Fi device types shown in this table, see [Non-Wi-Fi Interferers on page 2433](#).

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
freq-band {2.4ghz 5ghz}	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Example

The output of this example shows that the spectrum monitor **ap123** is able to detect 61 Wi-Fi devices on channel 149:

```
(host) [mynode] #show ap spectrum device-summary ap-name ap123 freq-band
5ghz

Device Summary Table
-----
Device                149   153   157   161   165
-----
Unknown                0     0     0     0     0
WIFI                   61    6    14    29    9
Microwave              0     0     0     0     0
Bluetooth              0     0     0     0     0
Generic Fixed Freq     0     0     0     0     0
Cordless Phone FF     0     0     0     0     0
Video                  0     0     0     0     0
```

```

Audio          0    0    0    0    0
Generic Freq Hopper 0    0    0    0    0
Cordless Phone FH 0    0    0    0    0
Xbox          0    0    0    0    0
Microwave Inverter 0    0    0    0    0
Total:12

```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum interference-power

```
show ap spectrum interference-power
  ap-name <ap-name>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  freq-band {2.4ghz | 5ghz | 6ghz}
  <chan-width>
```

Description

This command shows the interference power detected by a 802.11a or 802.11g radio on a spectrum monitor or hybrid AP. This table displays information about AP power levels, channel noise, and adjacent channel interference seen on each channel by a spectrum monitor or hybrid AP radio.

The output of this command displays the noise floor of each selected channel in dBm. The noise floor of a channel depends on the noise figure of the RF components used in the radio, temperature, presence of certain types of interferers or noise, and the width of the channel. For example, in a clean environment, the noise floor of a 20 MHz channel will be around -95 dBm and that of a 40 MHz channel will be around -92 dBm. Certain types of fixed frequency continuous transmitters such as video bridges, fixed frequency phones, and wireless cameras typically elevate the noise floor as seen by the Wi-Fi radio. Other interferers such as the frequency hopping phones, Bluetooth, and Xbox devices may not affect the noise floor of the radio. A Wi-Fi radio can only reliably decode Wi-Fi signals that are a certain dB above the noise floor and therefore estimating and understanding the actual noise floor of the radio is critical to understanding the reliability of the RF environment.

The ACI column displayed in the Interference Power Chart displays Adjacent-Channel Interference (ACI) power levels based on the signal strength(s) of the Wi-Fi APs on adjacent channels. A higher ACI value in Interference Power Chart does not necessarily mean higher interference since the AP that is contributing to the maximum ACI may or may not be very actively transmitting data to other clients at all times. The ACI power levels are derived from the signal strength of the beacons.

Parameter	Description
ap-name <ap-name>	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip-addr <ip-addr>	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
ip6-addr <ip6-addr>	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.

Parameter	Description
freq-band {2.4ghz 5ghz} (For versions prior to ArubaOS 8.9.0.0)	View information for a specific radio type, either 2.4 GHz or 5 GHz.
freq-band {2.4ghz 5ghz 6ghz} (For ArubaOS 8.9.0.0 or later versions)	View information for a specific radio type, either 2.4 GHz, 5 GHz, or 6 GHz. NOTE: The 6ghz sub-parameter is applicable to Wi-Fi 6E APs only.

Example

The output of this example shows interference power levels for each channel seen by the spectrum monitor **ap123**:

```
(host) [mynode] #show ap spectrum interference-power ap-name ap123 freq-band 5ghz

Interference Power Table
-----
Channel  Noise Floor (dBm)  Max AP Signal (dBm)  Max AP SSID  Max AP
BSSID    ACI (dBm)  Max Interference (dBm)  -----
-----
--
149      -91          -40                  ethersphere-wpa2
00:24:6c:80:7b:c9 -77          -71
153      -63          -42                  guest
00:1a:1e:87:c1:90 -63          -58
157      -92          -48                  alpha
00:1a:1e:50:01:30 -74          -60
161      -94          -39                  00:24:6C:C0:15:EB
00:24:6c:81:57:c8 -61          -70
165      -93          -26                  sw-jfb-attack
00:1a:1e:9b:1d:c8 -74          -69
149+     -60          -40                  ethersphere-wpa2
00:24:6c:80:7b:c9 -0           -58
157+     -89          -39                  00:24:6C:C0:15:EB
00:24:6c:81:57:c8 -0           -60
```

The output of this command includes the following information:

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Noise Floor (dBm)	Current noise floor recorded on the channel.
Max AP Signal (dBm)	Power level of the AP on the channel with the highest signal power.

Column	Description
Max AP SSID	SSID of the AP on the channel with the highest signal power.
Max AP BSSID	BSSID of the AP on the channel with the highest signal power.
ACI (dBm)	Adjacent channel interference level detected by the spectrum device.
Max Interference Power (dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.

Related Commands

Command	Description
<u>ap spectrum local-override</u>	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
<u>rf dot11a-radio-profilemodespectrum-mode</u>	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
<u>rf dot11g-radio-profilemodespectrum-mode</u>	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.9.0.0	The <code>6ghz</code> sub-parameter was introduced for <code>freq-band</code> parameter. (For ArubaOS 8.9.0.0 or later versions)
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum-load-balancing

```
show ap spectrum-load-balancing
  group <group>
```

Description

This command shows spectrum load balancing information for an AP with this feature enabled.

Parameter	Description
group <group>	Filter this information to show only data for the specified spectrum load balancing domain.

Example

The output of the command below shows the APs currently using the spectrum load-balancing domain **default-1**:

```
(host)[mynode] #show ap spectrum-load-balancing group default-1

Spectrum Load Balancing Group
-----
Name          IP Address      Domain      Assignment  Clients
-----
ap121-1      192.168.151.253 default-1   149/21      3
ap124-1      192.168.151.254 default-1   48/15      3
ap125-1      192.168.151.251 default-1   44/15      2
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.
IP address	IP address of the AP.
Domain	Name of the spectrum load balancing domain assigned to the AP.
Assignment	Current channel and power assignment for the AP.
Clients	Number of clients currently using the AP.

Related Commands

Command	Description
<u>ap spectrum local-override</u>	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
<u>rf dot11a-radio-profilemodespectrum-mode</u>	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
<u>rf dot11g-radio-profilemodespectrum-mode</u>	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum local-override

show ap spectrum local-override

Description

This command shows a list of AP radios currently converted to spectrum monitors through the spectrum local-override list.

Example

The output of this example shows that three APs each have two radios defined as spectrum monitors:

```
(host)[mynode] #show ap spectrum local-override
Spectrum Local Override Profile
-----
Parameter      Value
-----
Override Entry  AP ap125 band 2ghz
Override Entry  AP ap125 band 5ghz
Override Entry  AP ap105 band 2ghz
Override Entry  AP ap105 band 5ghz
Override Entry  AP apcorp1 band 2ghz
Override Entry  AP APcorp1 band 5ghz
```

The Value column in the output of this command includes the following information:

Parameter	Description
Override Entry	Indicates that an AP radio has been added to the local override list.
Value	Radio that has been added to the override list and the band used by that radio.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command	Description
<code>rf dot11g-radio-profilemode spectrum-mode</code>	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum monitors

```
show ap spectrum monitors
  ap-group <ap-group>
  ap-name <ap-name>
  ap-type <ap-type>
  channel <channel>
  freq-band <freq-band>
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
  or
  page <page>
  sort <sort>
```

Description

This command shows a list of APs terminating on the controller that are currently configured as spectrum monitors or hybrid APs.

Parameter	Description
ap-group <ap-group>	Specify the spectrum device's AP group.
ap-name <ap-name>	Specify the AP name configured as a spectrum monitor or hybrid AP.
ap-type <ap-type>	Specify the AP type.
channel <channel>	Specify the channel of hybrid monitor.
freq-band <freq-band>	Specify the frequency band.
ip-addr <ip-addr>	Specify the IP address of spectrum monitor.
ip6-addr <ip6-addr>	Specify the IPv6 address of spectrum monitor.
or	Show spectrum monitors that satisfy any of the given conditions:
page <page>	Enter a value greater than 1 for Page Number. The number of spectrum monitors displayed per page is 50.
sort <sort>	Sort criteria based on pairs of column name and order, e.g. ap-name,asc,channel,desc, and so on.

Example

The output of this example shows that the 802.11a radio on a spectrum monitor named **ap123** is sending spectrum analysis data to a client with the IP address 10.240.16.177.

```
(host) [mynode] #show ap spectrum monitors

List of Spectrum Monitors
-----
AP name          Group    AP Type  Phy  Band      Channel  Mode
-----
Client IP        Subscribe Time
-----
00:24:6c:c0:0c:89 default  105     G    2GHz      1         Access Point
00:24:6c:c0:0c:89 default  105     A    5GHz      44+       Access Point
10.240.16.177    2011-01-21 07:17:57 AM
00:24:6c:c7:d6:1c default  93      A    5GHz      -         Spectrum
Monitor 10.240.16.177 2011-01-21
07:18:22 AM
```

The output of this command includes the following information:

Column	Description
AP name	Name of an AP configured as a spectrum monitor or hybrid AP.
Group	Name of the spectrum device's AP group.
Ap Type	The AP model number .
Phy	The radio's PHY type. Possible values are A for 802.11a and G for 802.11b/g,
Band	Spectrum band that the spectrum monitor or hybrid AP radio is currently monitoring.
Mode	This column shows whether the device is an access point configured as a hybrid AP or a spectrum monitor.
Client IP	IP address of the client to which the spectrum monitor or hybrid AP is sending data.
Subscribe time	Time at which the spectrum monitor or hybrid AP was connected to the client.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.

Command	Description
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ■ ap-group ■ ap-name ■ ap-type ■ channel ■ freq-band ■ ip-addr ■ ip6-addr ■ sort
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum tech-support

```
show ap spectrum tech-support
  ap-name <ap-name>
  <filename>
```

Description

Saves spectrum data for later analysis by technical support. Use this command under the supervision of your Aruba technical support representative to troubleshoot spectrum analysis issues or errors.

Parameter	Description
ap-name <ap-name>	Saves technical support information for a specific spectrum monitor.
<filename>	Name of the file to which this data should be saved. This file does not have to already exist on the controller, the <code>show ap spectrum technical-support</code> command will create this file.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap standby

```
show ap standby
  ap-name <ap-name>
  bssid <bssid>
  details
  ip-addr <ip-addr>
  ip6-addr <ip6-addr>
```

Description

Shows all APs in standby mode currently registered to a managed device. This command displays details for all APs connected to a controller in standby mode.

Parameter	Description
ap-name <ap-name>	View data for an AP with a specified name.
bssid <bssid>	View data for a specific BSSID.
details	View AP data detailed columns.
ip-addr <ip-addr>	View data for an AP with a specified IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	View data for an AP with a specified IPv6 address.

Example

Issue the following command to view AP data detailed columns:

```
(host) [mynode] #show ap standby

Standby AP Table
-----
Name      Group      IP Address      AP Type  Flags  Uptime      Outer IP
Cluster  Role
-----  -
Radio 0  Band Ch/EIRP/MaxEIRP/Clients  Radio 1  Band Ch/EIRP/MaxEIRP/Clients
-----  -
Radio 2  Band Ch/EIRP/MaxEIRP/Clients
-----

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
A = Enet1 in active/standby mode; B = Battery Boost On; C = Cellular;
D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x
authentication;
H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M =
Mesh;
```

```

N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
S = AP connected as standby; X = Maintenance Mode;
a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert
RAP;
i = Provisioned as Indoor; o = Provisioned as Outdoor;
p = Restriction mode in POE-AF/AT;r = 802.11r Enabled; f = No Spectrum FFT
support;
Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz; t = Tri-Radio
Mode Enabled;
U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST
cert; W = Dual 5GHz Mode Enabled; 4 = Using WiFi Uplink
Channel followed by "*" indicates channel selected due to unsupported
configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.
Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz
(i.e. 36E+149E)
Cluster Role: U = UAC, A = AAC, SU = Standby UAC , SA = Standby AAC
Num APs:0

```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.6.0.0	A new output parameter <code>Radio 2 Band Ch/EIRP/MaxEIRP/Clients</code> and flag <code>t</code> were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap system-profile

show ap system-profile [<profile-name>]

Description

This command shows the system profile settings of an AP.

Parameter	Description
<profile-name>	Name of a system profile.

Example

The output of the command shows the current configuration settings for the default system profile:

```
(host) [mynode] #show ap system-profile default
AP system profile "default"
-----
Parameter
Value
-----
-----
RF Band
Recovery Mode
auto
RF Band for AM mode scanning
all
Native VLAN ID
WIDS AMPDU Optimization
Enabled
Tunnel Heartbeat Interval
Session ACL
ap-uplink-acl
Corporate DNS Domain
N/A
SNMP sysContact
N/A
LED operating mode (11n/11ac APs only)
normal
LED override
Disabled
Driver log level
warnings
Console log level
emergencies
SAP MTU
N/A
```

RAP MTU
1300 bytes
LMS IP
N/A
Backup LMS IP
N/A
LMS IPv6
N/A
Backup LMS IPv6
N/A
LMS Preemption
Disabled
LMS Hold-down Period
600 sec
LMS ping interval
20
Remote-AP DHCP Server VLAN
N/A
Remote-AP DHCP Server Id
192.168.11.1
Remote-AP DHCP Default Router
192.168.11.1
Remote-AP DHCP DNS Server
N/A
Remote-AP CORP DNS Server
N/A
Remote-AP CORP DNS Server IPV6
N/A
Remote-AP DHCP Pool Start
192.168.11.2
Remote-AP DHCP Pool End
192.168.11.254
Remote-AP DHCP Pool Netmask
255.255.255.0
Remote-AP DHCP Lease Time 0
days
Remote-AP uplink total bandwidth 0
kbps
Remote-AP bw reservation 1
N/A
Remote-AP bw reservation 2
N/A
Remote-AP bw reservation 3
N/A
Remote-AP Local Network Access
Disabled
Flex Radio Mode
5GHz
Dual 5GHz Mode
Automatic
Split-5GHz Mode
Disabled
IPM activation
Disabled
IPM power reduction steps with priorities
N/A

```

IPM Steps delete all
No
Bootstrap threshold 8
Double Encrypt
Disabled
Heartbeat DSCP 0
Management DSCP
N/A
IP DSCP to VLAN 802.1p priority mapping
N/A
Maintenance Mode
Disabled
Maximum Request Retries
10
Request Retry Interval
10 sec
Number of IPSEC retries
85
Secondary Master/Conductor IP/FQDN
N/A
AeroScout RTLS Server
N/A
RTLS Server configuration
N/A
RTLS Server Compatibility Mode
Enabled
SES-imagotag ESL Server IP
N/A
SES-imagotag ESL Server FQDN or IP address, higher priority than serverip
N/A
SES-imagotag ESL Channel
N/A
SES-imagotag ESL Radio Coexistence
Enabled
Slow Timer Recovery by rebooting itself
Enabled
Telnet
Disabled
Disable RAP Tftp Image Upgrade
Disabled
Image URL
N/A
Spanning Tree
Disabled
AP multicast aggregation
Disabled
AP ARP attack protection
Disabled
AP multicast aggregation allowed VLANs
none
Console enable
Enabled
AP Console Protection
Disabled
AP Console Password
*****

```



```

Password for Backup
*****
AP USB Power mode
auto
AP POE mode
shared
RF Band for Backup
all
Operation for Backup
off
BLE Operation Mode
Disabled
GRE offload
Enabled
Bridge offload
Enabled
Health Check
Disabled
Health Check Parameter
mode ping packet-size 32 burst-size 5 report 60 frequency 10 retries 3
Wired Port Down-Time By Shutdown Ethernet Link
40 sec
Wired Port Down-Time By Shutdown POE
30 sec
AirMatch Report Period
30 minutes
AirMatch Measurement Duration
minutes
AirMatch Report Enabled
Enabled
AP Deploy-hour
N/A
Dump collection profile
default

```

The output of this command includes the following information:

Column	Description
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: <ul style="list-style-type: none"> ▪ g = 2.4 GHz ▪ a = 5 GHz

Column	Description
Recovery Mode	Displays the AP behavior when a firmware assert is detected.
RF Band for AM mode scanning	Scanning band for multiple RF radios. <ul style="list-style-type: none"> ▪ g = 2.4 GHz ▪ a = 5 GHz ▪ all = Radio scans both bands. This is the default setting.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
WIDS AMPDU Optimization	Displays if the WIDS aggregate MPDU optimization is enabled or disabled.

Column	Description
Tunnel Heartbeat Interval	Interval between heartbeat messages between a remote or campus AP and its associated managed device. An increase in the heartbeat interval increases the time it will take for an AP to detect the loss in connectivity to the managed device, but can reduce Internet bandwidth consumed by a remote AP.
Session ACL	This parameter shows the ACL applied on the uplink of a remote AP.
Corporate DNS Domain	DNS name used by the corporate network.
SNMP sysContact	SNMP system contact information.
LED operating mode	Displays the LED operating mode for indoor 802.11n APs. LEDs display as usual in the default normal operating mode, but are all turned off in off mode.

Column	Description
	NOTE: If the LMS-IP is blank, the access point will remain on the managed device that it finds using methods like DNS or DHCP. If an IP address is configured for the LMS IP parameter, the AP will be immediately redirected to the managed device at that address.
Backup LMS IP	For networks with multiple managed devices, this parameter displays the IP address of a backup to the IP address specified with the lms-ip parameter.

Column	Description
LMS IPv6	For IPv6 networks with multiple managed devices, this parameter specifies the IPv6 address of the local management switch (LMS)—the Aruba managed device—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Conductor.
Backup LMS IPv6	In multi-controller IPv6 networks, this parameter specifies the IPv6 address of a backup to the IPv6 address specified with the LMS IPv6 setting.
LMS Preemption	When this parameter is enabled, the local management switch automatically reverts to the primary LMS IP address when it becomes available.

Column	Description
LMS Hold-down Period	<p>Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover. The <code>rap-dhcp-server-vlan</code> VLAN ID of the remote AP DHCP server is used if the managed device is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable.</p>
LMS ping interval	<p>The interval at which an application level ping is sent to a primary controller to check the reachability. Applicable only for RAPs.</p> <p>NOTE: If this parameter is changed, the UDP session timeout should be set accordingly on an intermediate router. The preferred timeout value is lms-ping-interval plus 30 seconds.</p>

Column	Description
Remote-AP DHCP Server VLAN	VLAN ID of the remote AP DHCP server used if the managed device is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN).
Remote-AP DHCP Server ID	IP address used as the DHCP server identifier.
Remote-AP DNS Server	IP address of the DNS server.
Remote-AP DHCP Default Router	IP address for the default DHCP router.
Remote-AP DHCP Pool Start	This parameter defines the starting IP address in the DHCP pool for remote APs.
Remote-AP DHCP Pool End	This parameter defines the last IP address in the DHCP pool for remote APs.
Remote-AP DHCP Pool Netmask	Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool.
Remote-AP uplink total bandwidth	This is the total reserved uplink bandwidth (in kilobits per second).

Column	Description
Remote-AP bw reservation 1 Remote-AP bw reservation 2 Remote-AP bw reservation 3	Session ACLs with uplink bandwidth reservation in kilobits per second. You can specify up to three session ACLs to reserve uplink bandwidth. The sum of the three uplink bandwidths should not exceed the rap-bw-total value.
Remote-AP Local Network Access	Shows if Remote-AP Local Network Access is enabled or disabled. By enabling this option, the clients that are connected to a remote AP can communicate. NOTE: By default, the Remote-AP Local Network Access will be disabled.
Flex Radio Mode	The mode for flexible radio.
Dual 5GHz Mode	The mode for dual 5 GHz APs.
Split-5GSHz Mode	The mode for split 5 GHz APs.

Column	Description
IPM activation	Displays the activation status of the Intelligent Power Monitoring (IPM) system.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP reboots. On the managed device, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Double Encrypt	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.

Column	Description
Dump Server	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
Heartbeat DSCP	DSCP value of AP heartbeats (0-63).
Maintenance Mode	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to the NMS or network operations centers when deploying, maintaining, or upgrading the network. The managed device still generates debug syslog messages if debug logging is enabled.
Maximum Request Retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.

Column	Description
Request Retry Interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.
Number of IPSEC retries	The number of times the AP will attempt to recreate an IPsec tunnel with Mobility Conductor before the AP will reboot. A value of 0 disables the reboot.
AeroScout RTLS Server	<p>This parameter contains the following information, separated by colons:</p> <ul style="list-style-type: none"> ▪ IPv4 or IPv6 address of an AeroScout real-time asset location (RTLS) server to which locations report are sent. ▪ Port number: Port number on the

Column	Description
	<p>AeroScout server to which location reports are sent.</p> <ul style="list-style-type: none"> ▪ Include-unassoc-sta: Specifies whether to include unassociated stations when sending station reports. Unassociated stations are stations that are not associated to any AP <p>Default: Disabled</p>
RTLS Server configuration	<p>This parameter contains the following information, separated by colons.</p> <ul style="list-style-type: none"> ▪ IPv4 or IPv6 address of the RTLS server to which the AP sends RFID tag information. ▪ Number of the RTLS server port to which the

Column	Description
	<p>AP sends RFID tag information.</p> <ul style="list-style-type: none"> ▪ Shared secret key for the server. ▪ Frequency at which packets are sent to the server, in seconds.
AP USB Power mode	<p>Displays the status of USB port on various AP platforms that have external USB ports. Listed below are the power modes:</p> <ul style="list-style-type: none"> ▪ auto: Detect USB power mode automatically. ▪ disable: Disable USB power. ▪ enable: Enable USB power. <p>NOTE: This parameter can be configured only on AP-214, AP-215, AP-224, AP-225, AP-205H, AP-303H, AP-304, AP-305, AP-314, AP-315, AP-324, AP-325, AP-334, AP-335, AP-344, AP-345, AP-203R, and AP-203RP access</p>

Column	Description
	points only.
Telnet	Reports whether telnet access to the AP is enabled or disabled.
RF Band for Backup	If the system profile is enabled, the AP console accesses using a backup ESSID.
Operation for Backup	This parameter allows AP console access using a backup ESSID, allowing users to access an AP console after the AP has disconnected from the managed device. When the AP advertises a backup ESSID in either static or dynamic mode, an user is able to access and debug the AP remotely through a virtual AP. This feature is disabled by default.
BLE Endpoint URL	Displays the URL of the Meridian server to which the Bluetooth Low Energy (BLE) sends monitoring data.

Column	Description
BLE Auth Token	Displays the BLE endpoint authorization token. This token is unique for each deployment.
BLE Operation Mode	Displays the BLE operation mode of the AP.
Wired Port Down-Time By Shutdown Ethernet Link	Displays the amount of time the AP needs to keep the Ethernet link of the wired port in down state after failover to backup cluster or fallback to primary cluster. NOTE: The port bounce feature is disabled when the value is 0.
Wired Port Down-Time By Shutdown POE	Displays the amount of time the AP needs to keep the PoE of the wired port in down state after failover to backup cluster or fallback to primary cluster. NOTE: The port bounce feature is disabled when the value is 0.

Starting from ArubaOS 8.2.0.0, the output of the `show ap system-profile <profile-name> | include IPM` command is modified to display a new output parameter, IPM Steps delete all.

```
(host) [mynode] #show ap system-profile default | include IPM
IPM activation                               Disabled
IPM power reduction steps with priorities    N/A
```


IPM Steps delete all No

Starting from ArubaOS 8.4.0.0, the output of the `show ap system-profile <profile-name> | include USB` command is modified to display a new output parameter, `AP USB Power mode`.

```
(host) [mynode] #show ap system-profile default | include USB
AP USB Power mode          auto
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.8.0.0	The following parameters were introduced in the command output: <ul style="list-style-type: none">■ <code>Wired Port Down-Time By Shutdown Ethernet Link</code>■ <code>Wired Port Down-Time By Shutdown POE</code>
ArubaOS 8.4.0.0	The following changes were introduced: <ul style="list-style-type: none">■ The output of the <code>show ap system-profile <profile-name> include USB</code> command displayed the <code>AP USB Power mode</code> parameter.■ The <code>AeroScout RTLS Server</code> and <code>RTLS Server</code> configuration output parameter of the <code>show ap system-profile <profile-name> include RTLS</code> command displayed IPv6 address.
ArubaOS 8.2.0.0	A new output parameter, <code>IPM Steps delete all</code> , was included in the output of the <code>show ap system-profile <profile-name> include IPM</code> command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap tech-support

```
show ap tech-support ap-name <ap-name> [<filename>]
```

Description

This command displays all information for an AP, or saves that information to a file on the controller. This information can be used by Aruba technical support to diagnose a problem with an AP. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with an AP or your wireless network.

Parameter	Description
<ap-name>	Name of the AP for which you want to view tech support data.
<filename>	Save the output of this command to a file on the controller with the specified filename.

Related Commands

Command	Description
show tech-support	This command displays all information about the controller required for technical support purposes.

Command History

Release	Modification
ArubaOS 8.8.0.0	The output of the command was modified to display Ethernet related details.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap vht-rates

```
show ap vht-rates bssid <bssid>
```

Description

Shows Very-High-Throughput (VHT) rates for an AP that supports 802.11ac.

Parameter	Description
bssid <bssid>	Shows VHT rates for a specific Basic Service Set Identifier (BSSID) on an 802.11ac-capable AP. The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP radio.

Example

The output of the command below shows very-high-throughput rates for 20 MHz, 40 MHz, and 80 MHz data streams with and without a Short Guard Interval (SGI).

```
(host) [mynode] #show ap vht-rates bssid 6c:f3:7f:e7:51:f0
AP "Corp-ac" Radio 0 BSSID 6c:f3:7f:e7:51:f0 Very-high-throughput Rates
(Mbps)
-----
--
MCS  Streams  20 MHz  20 MHz SGI  40 MHz  40 MHz SGI  80 MHz  80 MHz SGI
-----
0    1          6.5    7.2    13.5   15.0   29.3   32.5
1    1          13.0   14.4   27.0   30.0   58.5   65.0
2    1          19.5   21.7   40.5   45.0   87.8   97.5
3    1          26.0   28.9   54.0   60.0   117.0  130.0
4    1          39.0   43.3   81.0   90.0   175.5  195.0
5    1          52.0   57.8   108.0  120.0  234.0  260.0
6    1          58.5   65.0   121.5  135.0  263.3  292.5
7    1          65.0   72.2   135.0  150.0  292.5  325.0
8    1          78.0   86.7   162.0  180.0  351.0  390.0
9    1          --     --     180.0  200.0  390.0  433.3
0    2          13.0   14.4   27.0   30.0   58.5   65.0
1    2          26.0   28.9   54.0   60.0   117.0  130.0
2    2          39.0   43.3   81.0   90.0   175.5  195.0
3    2          52.0   57.8   108.0  120.0  234.0  260.0
4    2          78.0   86.7   162.0  180.0  351.0  390.0
5    2          104.0  115.6  216.0  240.0  468.0  520.0
6    2          117.0  130.0  243.0  270.0  526.5  585.0
7    2          130.0  144.4  270.0  300.0  585.0  650.0
8    2          156.0  173.3  324.0  360.0  702.0  780.0
9    2          --     --     360.0  400.0  780.0  866.7
0    3          19.5   21.7   40.5   45.0   87.8   97.5
1    3          39.0   43.3   81.0   90.0   175.5  195.0
2    3          58.5   65.0   121.5  135.0  263.3  292.5
3    3          78.0   86.7   162.0  180.0  351.0  390.0
```

```

4   3      117.0  130.0      243.0  270.0      526.5  585.0
5   3      156.0  173.3      324.0  360.0      702.0  780.0
6   3      175.5  195.0      364.5  405.0      --      --
7   3      195.0  216.7      405.0  450.0      877.5  975.0
8   3      234.0  260.0      486.0  540.0     1053.0 1170.0
9   3      260.0  288.9      540.0  600.0     1170.0 1300.0
-- : not valid.
Range for 20 MHz:  6.5 - 288.9 Mbps
Range for 40 MHz: 13.5 - 600.0 Mbps
Range for 80 MHz: 29.3 - 1300.0 Mbps

```

The output of this command includes the following information:

Output	Description
MCS	A Modulation Coding Scheme (MCS) values supported on this high-throughput SSID.
Streams	Number of spatial streams used by the MCS index value.
20 MHz	802.11n data rates for the MCS for 20 MHz transmissions.
20 MHz SGI	802.11n data rates for the MCS for 20 MHz transmissions using a short guard interval.
40 MHz	802.11n data rates for the MCS for 40 MHz transmissions.
40 MHz SGI	802.11n data rates for the MCS for 40 MHz transmissions using a short guard interval.
80 MHz	802.11n data rates for the MCS for 80 MHz transmissions.
80 MHz SGI	802.11n data rates for the MCS for 80 MHz transmissions using a short guard interval.

Related Commands

Command	Description
show ap ht-rates	Shows high-throughput rate information for a Basic Service Set (BSS).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
This command will only show rate information for 802.11ac-capable APs.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap virtual-beacon-report

```
show ap virtual-beacon-report {all | ap-name <ap-name> | client-mac <client-mac> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

If the Client Match feature is enabled, the output of this command displays the virtual beacon report for an AP or a client with a specific IP or MAC address. Use this command to display the client RSSI from the APs in its RF neighborhood, the channel used by each AP radio, and the number of clients associated to each radio.

Parameter	Description
all	Virtual beacon report for all clients on the controller.
ap-name <ap-name>	Name of the AP for which you want to view a virtual beacon report.
client-mac <client-mac>	MAC address of a client for which you want to view a virtual beacon report.
ip-addr <ip-addr>	IPv4 address of an AP for which you want to view a virtual beacon report.
ip6-addr <ip6-addr>	IPv6 address of an AP for which you want to view a virtual beacon report.

Examples

The following example displays the virtual beacon report for a client with MAC address 48:e2:44:b1:8a:95:

```
(host) [mynode] #show ap virtual-beacon-report client-mac 48:e2:44:b1:8a:95

Client MAC :48:e2:44:b1:8a:95
6GHz Capable: No
Current association :AP515-Desk-1 (9c:8c:d8:12:81:1f)
Steer attempts/Success :0/0
Consecutive (Fails/BTM Rej/BTM Timeouts) :0/0/0
Bandsteer window (Steers/Start time/Expiry time) :0/0/0
Client Device Type :
Client OS version:
Current state :Steerable
Active media sessions :No
Client Supported Channels :{1,13} {36,4} {52,4} {100,11} {144,1} {149,4}
{165,1}
Client Non-preferred Channels :None specified
Current Time :Dec 16 17:04:04 2019
```



```

STA Beacon Report
-----
AP          IP address          Radio          ESSID
Signal (dBm) Last update    Add time      Channel/EIRP/Clients
Flag
-          -----          -          -
--
AP515-Desk-1 2620:11d:6036:4a1:9e8c:d8ff:fec9:2810 9c:8c:d8:12:81:10
UofMWifi-dot1x -45          Dec 16 17:03:51 Dec 16 15:50:34 44/21.0/62
  *H
AP555-2-1    2620:11d:6036:4a1:828d:b7ff:fec0:ad4 80:8d:b7:80:ad:40
UofMWifi-dot1x -39          Dec 16 17:03:36 Dec 16 16:51:06 44/18.0/12
  H
1248-205     10.100.66.128          9c:1c:12:fe:19:e0
ethersphere-wpa2 -81          Oct 29 15:29:57 Oct 29 10:10:30 1/12/1
  S
1242-205     10.100.66.123          9c:1c:12:fd:d1:20
ethersphere-wpa2 -69          Oct 29 15:44:03 Oct 29 10:58:40 1/12/0
  S
VBR Flags *-Associated S-Stale U-Unsupported Channel

```

The output of this command includes the following parameters:

Parameter	Description
Client MAC	MAC address of the client.
Current association	MAC address of the AP radio to which the client is currently associated.
Steer attempts/Success	Number of steer attempts and the number of successful steers.
Consecutive (Fails/BTM Rej/BTM Timeouts)	Consecutive number of failed steer attempts, rejected BSS Transition Management Requests, and BSS Transition Management timeouts.
Bandsteer window (Steers/Start time/Expiry time)	Number of band steers, the start time of the band steer, and the expiry time of the band steer.
Client Device Type	Type of device used by the client (for example, Windows).
Current State	Indicates whether the client is currently steerable.

Parameter	Description
Client Supported Channels	Lists the channels that support client use.
Current Time	Timestamp showing the current date and time.
AP	Name of the AP from which the client can detect a signal.
IP address	IPv4 or IPv6 address of the AP from which the client can detect a signal.
Radio	MAC address of the AP radio from which the client can detect a signal.
ESSID	Identifying name of the wireless network for each AP.
Signal (dBm)	Signal strength, in dBm, from the AP radio.
Last Update	Time that the virtual beacon report last updated information for the AP radio.
Add Time	Date and time the client is successfully steered and added to the AP.
Channel/EIRP/Clients	Channel used by the AP radio, the amount of power transmitted from the AP antennae, and the number of clients associated to it.
Flag	<p>The output of this column shows the following values:</p> <ul style="list-style-type: none"> ▪ *: Flag indicating that the client is currently associated to this AP ▪ S: Flag indicating a stale entry, with the last client update from this radio produced 120+ seconds ago ▪ U: Flag indicating that the client does not support the channel the radio is currently operating on

The following example displays a virtual beacon report for all clients in the network:

```
(host) [mynode] #show ap virtual-beacon-report all
```

```

Client MAC :60:d9:c7:a2:42:cb
Current association :1260-205 (9c:1c:12:fe:0f:d2)
Steer attempts/Success :0/0
Consecutive (Fails/BTM Rej/BTM Timeouts) :0/0/0
Bandsteer window (Steers/Start time/Expiry time) :0/0/0
Client Device Type :Unknown
Current state :Steerable
Active media sessions: No
Client Supported Channels :{36,4}{52,4}{100,11}{149,4}{165,1}
Current Time :Oct 29 12:38:35 2014

```

STA Beacon Report

```

-----
AP          IP address      Radio          ESSID          Signal (dBm)
Last update  Add time       Channel/EIRP/Clients  Flag
--          -
-----
1372-205    10.100.66.120  9c:1c:12:fe:13:50  ethersphere-psk  -67
Oct 29 12:38:22  Oct 29 07:19:33  52/21/10
1260-205    10.100.66.100  9c:1c:12:fe:0f:d0  ethersphere-psk  -53
Oct 29 12:38:18  Oct 29 07:19:44  52/24/15          *
1263-ac     10.100.66.121  6c:f3:7f:e7:5a:b0  ethersphere-psk  -73
Oct 29 07:20:52  Oct 29 07:19:49  52/12/5           S
1362-205    10.100.66.127  9c:1c:12:fd:f2:30  ethersphere-psk  -73
Oct 29 07:57:21  Oct 29 07:52:31  60/12/12          S
1310-205    10.100.66.102  9c:1c:12:fd:f7:b0  ethersphere-psk  -80
Oct 29 10:36:15  Oct 29 07:52:51  44/20/34          S
1263-205    10.100.66.126  9c:1c:12:fd:d2:10  ethersphere-psk  -67
Oct 29 08:42:20  Oct 29 08:22:32  60/12/4           S

```

The output of this command includes the additional `Active Media Sessions` parameter, which indicates whether the client is involved in any active media sessions.

Related Commands

Command	Description
rf arm-profile	Configures the Adaptive Radio Management (ARM) profile.
show ap arm client-match probe-report	Displays additional statistics for the Client Match feature.
show ap arm client-match restriction-table	Displays additional statistics for the Client Match feature.

Command History

Release	Description
ArubaOS 8.7.0.0	The output of the command was modified to also display 6 GHz capable.
ArubaOS 8.7.0.0	The output of the command was modified to also display IPv6 address of the AP.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap vlan-mcast

```
show ap vlan-mcast [{ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}]
```

Description

This command shows the user count in each VLAN and timestamps for tunnel to join or leave vlan-mcast group.

Parameter	Description
ap-name <ap-name>	Show user count VLAN data for a specific AP name.
bssid <bssid>	Show user count VLAN data for a specific MAC address.
ip-addr <ip-addr>	Show user count VLAN data for a specific IP address.
ip6-addr <ip6-addr>	Show user count VLAN data for a specific IPv6 address.

Example

Use the following command to show the user count in each VLAN:

```
(host)[mynode] #show ap vlan-mcast
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap usb-acl-prof

```
show ap usb-acl-prof {default}{profile-name}
```

Description

This command shows the AP USB profile.

Parameter	Description
default	Shows the default AP USB ACL profile.
<profile-name>	Shows the AP USB profile.

Examples

The following command shows the list of USB ACL profiles:

```
(host) [mynode] #show ap usb-acl-prof

AP USB ACL profile List
-----
Name           References  Profile Status
----           -
sample         1
default        0

Total: 2
The following command shows the details of an USB ACL profile:
(host) (mynode) #show ap usb-acl-prof default

AP USB ACL profile "default"
-----
Parameter      Value
-----
AP USB ACL Config  N/A
```

Related Commands

Command	Description
ap usb-acl-prof	Configures AP USB ACL profile.
ap usb-profile	Configures AP USB profile.
show ap usb-prof	Shows configuration for AP USB profile.

Command	Description
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable Mode.

show ap usb-device-mgmt

```
show ap usb-device-mgmt all|{ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{wired mac <wired mac>}
```

Description

This command shows the USB devices managed on an AP.

Parameter	Description
all	Show all managed USB devices.
ap-name <ap-name>	Show USB devices managed on an AP that is specified by the AP name.
ip-addr <ip-addr>	Show USB devices managed on an AP that is specified by the IP address.
ip6-addr <ip6-addr>	Show USB devices managed on an AP that is specified by the IPv6 address.
wired mac <wired mac>	Show USB devices managed on an AP that is specified by the MAC address.

Example

The following command shows the list of all managed USB devices:

```
(host) [mynode] #show ap usb-device-mgmt all

USB Device
-----
Device ID  AP mac  Vender ID  Product ID  Manufacturer  Product  Version
Serial Number  Class  Device  Driver  Uptime
-----  -----  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----  -----
```

Related Commands

Command	Description
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.

Command	Description
show ap usb-prof	Shows configuration for AP USB profile.
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
ap usb-acl-prof	Configures AP USB ACL profile.
ap usb-profile	Configures AP USB profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable Mode.

show ap usb-prof

show ap usb-prof default | usb-profile

Description

This command shows the AP USB profile.

Parameter	Description
default	Show the default AP USB profile.
usb-profile	Show the AP USB profile.

Examples

The following command shows the list of AP USB profiles:

```
(host) [mynode] #show ap usb-profile

AP USB profile List
-----
Name           References  Profile Status
----           -
default        3
sample        0

Total: 2
```

The following command shows the details of an AP USB profile:

```
(host) [mynode] #show ap usb-profile default

AP USB profile "default"
-----
Parameter          Value
-----
AP USB ACL Profile N/A
```

Related Commands

Command	Description
ap usb-profile	Configures AP USB profile.

Command	Description
ap usb-acl-prof	Configures AP USB ACL profile.
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable Mode.

show ap usb verbose

```
show ap usb verbose {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows the details of Aruba USB modem.

Parameter	Description
ap-name <name>	Shows data for an AP with a specific name.
ip-addr <ipaddr>	Shows data for an AP with a specific IPv4 address.
ip6-addr <ip6-addr>	Shows data for an AP with a specific IPv6 address.

Example

The following command shows the details of an AP USB profile.

```
(host) [mynode] (config) #show ap usb verbose ap-name 20:4c:03:a4:a6:85
T: Bus=06 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#= 1 Spd=5000 MxCh= 1
B: Alloc= 0/800 us ( 0%), #Int= 0, #Iso= 0
D: Ver= 3.00 Cls=09(hub ) Sub=00 Prot=03 MxPS= 9 #Cfgs= 1
P: Vendor=1d6b ProdID=0003 Rev= 4.01
S: Manufacturer=Linux 4.1.52 xhci-hcd
S: Product=xHCI Host Controller
S: SerialNumber=xhci-hcd.0
C:* #Ifs= 1 Cfg#= 1 Atr=e0 MxPwr= 0mA
I:* If#= 0 Alt= 0 #EPs= 1 Cls=09(hub ) Sub=00 Prot=00 Driver=hub
E: Ad=81(I) Atr=03(Int.) MxPS= 4 Ivl=256ms
T: Bus=05 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#= 1 Spd=480 MxCh= 0
B: Alloc= 0/800 us ( 0%), #Int= 0, #Iso= 0
D: Ver= 2.00 Cls=09(hub ) Sub=00 Prot=01 MxPS=64 #Cfgs= 1
P: Vendor=1d6b ProdID=0002 Rev= 4.01
S: Manufacturer=Linux 4.1.52 xhci-hcd
S: Product=xHCI Host Controller
S: SerialNumber=xhci-hcd.0
C:* #Ifs= 1 Cfg#= 1 Atr=e0 MxPwr= 0mA
I:* If#= 0 Alt= 0 #EPs= 1 Cls=09(hub ) Sub=00 Prot=00 Driver=(none)
E: Ad=81(I) Atr=03(Int.) MxPS= 4 Ivl=256ms
T: Bus=04 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#= 1 Spd=12 MxCh= 1
B: Alloc= 0/900 us ( 0%), #Int= 0, #Iso= 0
D: Ver= 1.10 Cls=09(hub ) Sub=00 Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=1d6b ProdID=0001 Rev= 4.01
S: Manufacturer=Linux 4.1.52 ohci_hcd
S: Product=Generic Platform OHCI controller
S: SerialNumber=ohci-platform.1
C:* #Ifs= 1 Cfg#= 1 Atr=e0 MxPwr= 0mA
I:* If#= 0 Alt= 0 #EPs= 1 Cls=09(hub ) Sub=00 Prot=00 Driver=hub
E: Ad=81(I) Atr=03(Int.) MxPS= 2 Ivl=255ms
```

Related Commands

Command	Description
ap usb-profile	Configures AP USB profile.
ap usb-acl-prof	Configures AP USB ACL profile.
show ap usb-acl-prof	Shows configuration for AP USB ACL profile.
show ap usb-device-mgmt	Shows USB devices managed on an AP.
show ap debug usb-device-mgmt	Shows debugging information of USB devices managed on an AP.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable Mode.

show ap vlan-usage

```
show ap vlan-usage [{ap-name <ap-name> | bssid <bssid> | essid <ssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr> | virtual-ap <virtual-ap>}
```

Description

Shows the number of clients on each VLAN.

Parameter	Description
ap-name <ap-name>	Show VLAN data for an AP with a specific name.
bssid <bssid>	Show VLAN data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP.
ssid <ssid>	Show VLAN data for a specific Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
ip-addr <ip-addr>	Show VLAN data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show VLAN data for an AP with a specific IPv6 address by entering an IP address in dotted-decimal format.
virtual-ap <virtual-ap>	Show VLAN pool allocation by VAP name.

Examples

The output of this command displays the **VLAN Usage** table :

```
(host) [mynode] #show ap vlan-usage
VLAN Usage Table
-----
VLAN ID  Clients
-----  -
64       1
65       32
66       44
```

The output of this command includes the following information:

Output	Description
VLAN ID	ID number of the wireless VLAN.
Clients	Number of clients currently using the specified VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wifi-uplink blacklist/ show ap wifi-uplink denylist

```
show ap wifi-uplink blacklist / show ap wifi-uplink denylist {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows a list of Wi-Fi uplink APs that have been denied access. The optional output modifiers | begin | exclude | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP that has been blocked.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the blocked AP.

Example

The following example displays the output of the blacklist/denylist command:

```
(host) [md] #show ap wifi-uplink blacklist/show ap wifi-uplink denylist ip-addr 10.65.43.247
WiFi uplink candidates
-----
essid bssid channel rssi encryption phy block-time remaining-time
(sec) reason
-----
-
Total blacklist/denylist:0; Current time: 2019-02-27 19:51:45
(host) [md] #show ap wifi-uplink blacklist/show ap wifi-uplink denylist ip-addr 10.65.43.247
WiFi uplink candidates
-----
essid bssid channel rssi encryption phy block-time remaining-time
(sec) reason
-----
-
Total blacklist/denylist:0; Current time: 2019-02-27 19:51:45
```

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink candidates

```
show ap wifi-uplink candidates {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows a list of Wi-Fi uplink candidate APs. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the candidate AP for Wi-Fi client. Default: AP name.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the candidate AP for Wi-Fi client.

Example

The following example displays the output of an uplink candidate. (For versions prior to ArubaOS 8.10.0.0)

```
(host) [mynode] #show ap wifi-uplink candidates ip-addr 10.65.43.247
WiFi uplink candidates
-----
essid          bssid          channel  rssi  encryption  phy      rank
up time       last update (total updates)
-----
-----
gran-uplink   ac:a3:1e:d2:19:d0  36      51    WPA2-psk    VHT-3ss  0/0/0/0
8h:40m:20s   2019-02-28 04:15:11 (551440)
Total candidates:1; Current time: 2019-02-28 04:15:11
```

The following example displays the output of an uplink candidate for a Wi-Fi 6E AP (ArubaOS 8.10.0.0 or later versions).

```
(host) [mynode] #show ap wifi-uplink candidates ap-name ap655-8391
WiFi uplink candidates
-----
essid          bssid          channel  band  rssi  encryption  phy
rank          up time       last update (total updates)
-----
-----
-----
```

```

test-wifi-wpa3 1c:28:af:68:2a:70 37 6GHz 210? WPA3 HE-2ss
61906/0 2d:13h:37m:49s 2021-07-28 12:45:58 (94685)
test-wifi-wpa3 1c:28:af:68:2a:80 161 5GHz 128? WPA3 HE-2ss
61312/0 1d:6h:47m:5s 2021-08-14 10:39:08 (2)
Total candidates:2; Current time: 2021-07-14 05:05:27

```

The output of this command includes the following information:

Output	Description
ssid	Name of the required ESSID to which the client is associated.
bssid	Name of the required BSSID to which the client is associated.
channel	The radio channel used by the AP.
band	The radio band used by the AP.
rsssi	The Received Signal Strength Indicator (RSSI) of the AP radio.
encryption	The encryption type used on the AP.
phy	The AP association for the specified PHY radio type (2.4 GHz, 5 GHz, or 6 GHz).
rank	The rank details of the AP.
up time	Number of hours, minutes and seconds since the discovered AP starts the BSS service or advertises the beacon, in the format hours:minutes:seconds.
last update (total updates)	Date and time stamp of the last AP update.

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.10.0.0	The command output was modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ 6GHz value for <code>band</code> parameter.

Command	Description
	<ul style="list-style-type: none"> ■ WPA3 value for <code>encryption</code> parameter.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink connection-history

```
show ap wifi-uplink connection-history {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows the connection history of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example shows the output of a connection history of a Wi-Fi uplink AP. (For versions prior to ArubaOS 8.10.0.0.)

```
(host) [mynode] #show ap wifi-uplink connection-history ip-addr 10.65.43.247
WiFi uplink connection history
-----
timestamp          essid          bssid          channel  rssi  result
-----
2019-02-27 19:37:41 gran-uplink    ac:a3:1e:d2:19:d0 36      51    SUCCESS
2019-02-28 05:01:12 gran-uplink    ac:a3:1e:d2:19:d0 149     52    SUCCESS
Total connection times:2; Current time: 2019-02-28 12:51:35
```

The following example shows the output of a connection history of AP-655 access point with Wi-Fi uplink enabled (ArubaOS 8.10.0.0 or later versions).

```
(host) [mynode] #show ap wifi-uplink connection-history ap-name ap655-8391
WiFi uplink connection history
-----
timestamp          essid          bssid          channel  band  rssi
result
-----
-----
2021-07-14 04:48:59 test-wifi-wpa3 1c:28:af:68:2a:70 37      6GHz  178
SUCCESS
Total connection times:1; Current time: 2021-07-14 05:03:15
```

The output of this command includes the following information:

Output	Description
timestamp	The date and time when the entry was created.
ssid	Name of the required ESSID to which the client is associated.
bssid	Name of the required BSSID to which the client is associated.
channel	The radio channel used by the AP.
band	The radio band used by the AP.
rssi	The Received Signal Strength Indicator (RSSI) of the AP radio.
result	The success or failure status of the connection.

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.10.0.0	The command output was modified to display 6GHz value for <code>band</code> parameter on Wi-Fi 6E APs.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink connection-trace

```
show ap wifi-uplink connection-trace {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows the connection trace of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example shows the output of a connection trace:

```
(host) [mynode] #show ap wifi-uplink connection-trace ip-addr 10.65.45.61
WiFi uplink connection trace
-----
2019-02-27 19:37:41  auth          -> 40:e3:d6:7f:2c:90  ac:a3:1e:d2:19:d0
  retry=no; tries=0; status=success
2019-02-27 19:37:41  auth          <- 40:e3:d6:7f:2c:90  ac:a3:1e:d2:19:d0
  SN=1964; retry=no; status=0
2019-02-27 19:37:41  assoc req     -> 40:e3:d6:7f:2c:90  ac:a3:1e:d2:19:d0
  retry=no; tries=0; status=success
2019-02-27 19:37:41  assoc resp    <- 40:e3:d6:7f:2c:90  ac:a3:1e:d2:19:d0
  SN=1965; retry=no; status=0
2019-02-27 19:37:41  connection up *
  bssid=ac:a3:1e:d2:19:d0
2019-02-27 19:37:41  eapol-key     <- 40:e3:d6:7f:2c:90  ac:a3:1e:d2:19:d0
  ver=1; len=117
```

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink current-profile

```
show ap wifi-uplink current-profile {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows the current profile information of APs with Wi-Fi uplink. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example shows the uplink profile priority:

```
(host) [mynode] #show ap wifi-uplink current-profile ip-addr 10.65.45.61
ap wifi-uplink profile "gran-uplink" priority 1
-----
Item                               Value
----                               -
ESSID                               gran-uplink
BSSID                               ac:a3:1e:d2:19:d0
Allowed band                         a
Encryption                           personal
WEP Key 1                            *****
WEP Key 2                            *****
WEP Key 3                            *****
WEP Key 4                            *****
WEP Transmit Key Index              1
WPA Hexkey                           *****
WPA Passphrase                        *****
```

The output of this command includes the following information:

Output	Description
ESSID	Name of this instance of the profile.
BSSID	Name of the required BSSID to which the client is associated.
Allowed band	The radio band(s) on which the Wi-Fi uplink is used: <ul style="list-style-type: none"> ▪ a: 802.11a band only (5 GHz) ▪ g: 802.11g band only (2.4 GHz) ▪ all: Both 802.11a and 802.11g bands (5 GHz and 2.4 GHz)
Encryption	Name of the required BSSID to which the client is associated.
WEP Key 1	The first static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 2	The second static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 3	The third static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 4	The fourth static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Transmit Key Index	The key index to specify which static WEP key is to be used. Can be 1, 2, 3, or 4.
WPA Hexkey	The WPA Pre-Shared Key (PSK).
WPA Passphrase	The WPA password that generates the PSK.

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink debug

```
show ap wifi-uplink debug
  mat-table {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
  supplicant-log {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
  wcd-debug-log {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
  wcd-error-log {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Show debug information of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
mat-table	MAC address translation table of Wi-Fi uplink. This parameter has the following sub-parameters: <ul style="list-style-type: none">▪ ap-name <ap-name> Name of the AP with Wi-Fi client.▪ bssid <bssid> Name of the required BSSID of the AP.▪ ip-addr <ip-addr> IP address of the AP with Wi-Fi client.
supplicant-log	Supplicant log information. This parameter has the following sub-parameters: <ul style="list-style-type: none">▪ ap-name <ap-name> Name of the AP with Wi-Fi client.▪ bssid <bssid> Name of the required BSSID of the AP.▪ ip-addr <ip-addr> IP address of the AP with Wi-Fi client.
wcd-debug-log	Debug log information of wcd process. This parameter has the following sub-parameters: <ul style="list-style-type: none">▪ ap-name <ap-name> Name of the AP with Wi-Fi client.▪ bssid <bssid> Name of the required BSSID of the AP.▪ ip-addr <ip-addr> IP address of the AP with Wi-Fi client.
wcd-error-log	Error log information of wcd process. This parameter has the following sub-parameters: <ul style="list-style-type: none">▪ ap-name <ap-name> Name of the AP with Wi-Fi client.▪ bssid <bssid> Name of the required BSSID of the AP.▪ ip-addr <ip-addr> IP address of the AP with Wi-Fi client.

Example

The following command displays the debug log of wcd process for an AP with Wi-Fi uplink:

```
(host) [mynode] #show ap wifi-uplink debug wcd-error-log ip-addr 10.65.45.61
[3101]2019-02-28 05:01:30.937 Internal error at file [wcd_wlan.c] function
[handle_connection_down] line [1572]
[3101]2019-02-28 13:00:00.100 Internal error at file [wcd_msg.c] function
[wcd_papi_rcv_cb] line [504] error: failed to send AMAPI result 0x1f8d6ac
50633
[3101]2019-02-28 13:00:20.118 Internal error at file [wcd_msg.c] function
[wcd_papi_rcv_cb] line [504] error: failed to send AMAPI result 0x1f8d6ac
50633
[3101]2019-02-28 13:00:40.136 Internal error at file [wcd_msg.c] function
[wcd_papi_rcv_cb] line [504] error: failed to send AMAPI result 0x1f8d6ac
50633
[3101]2019-02-28 13:01:08.182 Internal error at file [wcd_msg.c] function
[wcd_papi_rcv_cb] line [504] error: failed to send AMAPI result 0x1f8d6ac
50633
[3101]2019-02-28 13:01:28.202 Internal error at file [wcd_msg.c] function
[wcd_papi_rcv_cb] line [504] error: failed to send AMAPI result 0x1f8d6ac
50633
```

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink neighbors

```
show ap wifi-uplink neighbors {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows information of neighboring APs by scanning them. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example displays the information of neighboring APs with Wi-Fi uplink. (For versions prior to ArubaOS 8.10.0.0).

```
(host) [mynode] #show ap wifi-uplink neighbors ip-addr 10.65.45.61
WiFi uplink neighbors
-----
essid          bssid          channel  rssi  encryption
phy           up-time       last update (total updates)
-----
---
test001        00:00:00:80:00:00  36E      48    WPA2-psk
VHT-1ss       15s           2019-02-28 05:01:09(51232)
84:d4:7e:d2:80:10  116E          9      WPA2-psk
VHT-4ss       14h:59m:26s   2019-02-28 04:53:20(172)
aaa3          18:64:72:7f:60:10  100E     41    opensystem
VHT-4ss       29d:18h:27m:43s 2019-02-28 05:01:10(52716)
aaa4          18:64:72:7f:60:11  100E     44    opensystem
VHT-4ss       29d:18h:27m:43s 2019-02-28 05:01:10(52626)
ethersphere-wpa2-instant 84:d4:7e:d2:80:12  116E          9      WPA2-enterprise
VHT-4ss       15h:7m:16s     2019-02-28 05:01:10(142)
0000ppsk-tkip 18:64:72:7f:60:12  100E     44    WPA2-enterprise
VHT-4ss       29d:18h:27m:43s 2019-02-28 05:01:10(53718)
```

The following example displays the information of neighboring Wi-Fi 6E APs with Wi-Fi uplink (ArubaOS 8.10.0.0 or later versions).

```
(host) [mynode] #show ap wifi-uplink neighbors ap-name ap655-8391
WiFi uplink neighbors
-----
essid          bssid          channel band  rssi  encryption
phy    up time          last update (total updates)
-----
---
x-airwave-555  bc:9f:e4:2c:c0:20  48      5GHz  128?  WPA2-psk
HE-8ss  47d:8h:42m:31s  2021-08-14 10:39:03(1)
test-wifi-wpa3 1c:28:af:68:2a:70  37      6GHz  220?  WPA3
HE-2ss  2d:13h:32m:39s  2021-07-28 12:35:38(64393)
207-1x-ex      80:8d:b7:3f:5a:f2  132     5GHz  128?  WPA2-enterprise
legacy  20d:3h:1m:22s   2021-08-14 10:39:06(1)
test-wifi-1x   e8:26:89:09:de:d1  132     5GHz  0?    WPA2-enterprise
HE-2ss  1d:3h:20m:16s  2021-08-14 10:39:06(3)
test-wifi-open e8:26:89:09:de:d5  132     5GHz  112?  opensystem
HE-2ss  1d:3h:20m:16s  2021-08-14 10:39:06(3)
Total neighbours:5; Current time: 2021-07-14 05:00:16
```

The output of this command includes the following information:

Output	Description
essid	Name of the required ESSID to which the client is associated.
bssid	Name of the required BSSID to which the client is associated.
channel	The radio channel used by the AP.
band	The radio band used by the AP.
rssi	The Received Signal Strength Indicator (RSSI) of the AP radio.
encryption	The encryption type used on the AP.
phy	The AP association for the specified PHY radio type (802.11a or 802.11g)
up-time	Number of hours, minutes and seconds since the discovered AP starts the BSS service or advertises the beacon, in the format hours:minutes:seconds.
last update (total updates)	Date and time stamp of the last AP update.

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.10.0.0	The command output was modified to display the following changes on Wi-Fi 6E APs: ▪ 6GHz value for <code>band</code> parameter. ▪ WPA3 value for <code>encryption</code> parameter.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink-profile

```
show ap wifi-uplink-profile [<profile-name>]
```

Description

Shows a list of all Wi-Fi uplink profiles, or displays the configuration parameters in a specific Wi-Fi uplink profile. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	Name of a Wi-Fi uplink profile.

Example

The following example shows the configuration parameters for the Wi-Fi uplink profile "default". (For versions prior to ArubaOS 8.10.0.0).

```
(host) [mynode] #show ap wifi-uplink-profile default
WiFi uplink profile "default"
-----
Parameter          Value
-----
ESSID               aruba-ap
BSSID              N/A
Allowed band       all
Encryption         opensystem
WEP Key 1          N/A
WEP Key 2          N/A
WEP Key 3          N/A
WEP Key 4          N/A
WEP Transmit Key Index 1
WPA Hexkey         N/A
WPA Passphrase     *****
```

The following example shows the 6GHz configuration parameters for the Wi-Fi uplink profile "wpa3-transitioned". (ArubaOS 8.10.0.0 or later versions).

```
(host) [mynode] #show ap wifi-uplink-profile wpa3-transitioned
WiFi uplink profile "wpa3-transitioned"
-----
Parameter          Value
-----
ESSID              wpa3-transitioned
BSSID              N/A
```

```

RF band                6GHz
Encryption             personal
WEP Key 1              N/A
WEP Key 2              N/A
WEP Key 3              N/A
WEP Key 4              N/A
WEP Transmit Key Index 1
WPA Hexkey             N/A
WPA Passphrase        *****

```

The output of this command includes the following information.

Output	Description
ESSID	Name of the required ESSID to which the client is associated.
BSSID	Name of the required BSSID to which the client is associated.
Allowed band (For versions prior to ArubaOS 8.10.0.0)	<p>The radio band(s) on which the Wi-Fi uplink is used.</p> <ul style="list-style-type: none"> ▪ a—Supports 802.11a band only (5 GHz) ▪ g—Supports 802.11g band only (2.4 GHz) ▪ all—Supports both 802.11a and 802.11g bands (5 GHz and 2.4 GHz)
RF Band (ArubaOS 8.10.0.0 or later versions)	<p>The radio band(s) on which the Wi-Fi uplink is used.</p> <ul style="list-style-type: none"> ▪ a—Supports 802.11a band only (5 GHz) ▪ g—Supports 802.11g band only (2.4 GHz) ▪ 6GHz—Supports 6 GHz band only ▪ all—Supports 2.4 GHz, 5 GHz, and 6 GHz bands
Encryption	<p>Name of the data encryption mode.</p> <ul style="list-style-type: none"> ▪ opensystem— No authentication or encryption. ▪ personal— A wildcard

Output	Description
	<p>mode that matches several PSK mode key management suites and cipher suites, including WPA-PSK-TKIP, WPA-PSK-AES, WPA2-PSK-TKIP, WPA2-PSK-AES, and WPA3-SAE-AES.</p> <ul style="list-style-type: none"> ▪ static-wep— WEP with static keys. <p>NOTE: WPA3-SAE-AES encryption mode is supported for Wi-Fi 6E APs only (ArubaOS 8.10.0.0 or later versions).</p>
WEP Key 1	The first static WEP key associated with this key index.
WEP Key 2	The second static WEP key associated with this key index.
WEP Key 3	The third static WEP key associated with this key index.
WEP Key 4	The fourth static WEP key associated with this key index.
WEP Transmit Key Index	The key index to specify which static WEP key is to be used. Can be 1, 2, 3, or 4.
WPA Hexkey	A WPA Pre-Shared Key (PSK).
WPA Passphrase	The WPA password that generates the PSK.

Related Command

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The command output was modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ 6GHz value for <code>Allowed band</code> parameter. ■ WPA3-SAE-AES value for <code>Encryption</code> parameter.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wifi-uplink provisioned-profiles

```
show ap wifi-uplink provisioned-profiles {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows information of provisioned profiles of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following command displays the information of neighboring APs with Wi-Fi uplink:

```
(host) [mynode] #show ap wifi-uplink provisioned-profiles ip-addr
10.65.45.61
ap wifi-uplink profile <profile-name> priority 1
-----
Item                               Value
----                               -
ESSID                               gran-uplink
BSSID                               ac:a3:1e:d2:19:d0
Allowed band                         a
Encryption                           personal
WEP Key 1                            *****
WEP Key 2                            *****
WEP Key 3                            *****
WEP Key 4                            *****
WEP Transmit Key Index              1
WPA Hexkey                           *****
WPA Passphrase                        *****
```

The output of this command includes the following information:

Output	Description
ESSID	Name of this instance of the profile.
BSSID	Name of the required BSSID to which the client is associated.
Allowed band	The radio band(s) on which the Wi-Fi uplink is used: <ul style="list-style-type: none"> ▪ a: 802.11a band only (5 Ghz) ▪ g: 802.11g band only (2.4 Ghz) ▪ all: Both 802.11a and 802.11g bands (5 GHz and 2.4 GHz)
Encryption	Name of the required BSSID to which the client is associated.
WEP Key 1	The first static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 2	The second static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 3	The third static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Key 4	The fourth static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
WEP Transmit Key Index	The key index to specify which static WEP key is to be used. Can be 1, 2, 3, or 4.
WPA Hexkey	The WPA Pre-Shared Key (PSK).
WPA Passphrase	The WPA password that generates the PSK.

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink stats

```
show ap wifi-uplink stats {ap-name <ap-name> | ip-addr <ip-addr>}
```

Description

Shows the statistics of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example displays the statistics of the counters for the AP with Wi-Fi uplink profile:

```
(host) [mynode] #show ap wifi-uplink stats ip-addr 10.65.43.247
WiFi uplink stats
-----
Counter                               Value
-----
-----
General
-----
Transmit
Tx Frames Rcvd                         1154
Tx Bcast Frames Rcvd                   14
Tx Frames Dropped                       3
Tx Bcast Frames Dropped                 0
Tx Frames Transmitted                  1130
Tx Bytes Rcvd                          587606
Tx Bytes Transmitted                   585488
Tx Time Frames Rcvd                    180760
Tx Time Frames Dropped                  88
Tx Time Frames Transmitted              130440
Tx Success With Retry                   1143
Tx Multiple Retries                     1143
Tx Mgmt Frames                          13
Tx Beacons Transmitted                  0
Tx Probe Responses                      0
Tx Data Transmitted Retrieved           1143
Tx Data Transmitted                     1092
Tx Data Frames                          1095
Tx Broadcast Data Frames In             14
Tx Data Bytes Transmitted               563776
Tx Data Bytes                           587034
```


Tx Time Data Transmitted	127796
Tx Time BC/MC Data	3244
Tx Time Data dropped	88
Tx Time Data	171204

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wifi-uplink status

```
show ap wifi-uplink status {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr>}
```

Description

Shows the status of APs with Wi-Fi uplink. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ap-name <ap-name>	Name of the AP with Wi-Fi client.
bssid <bssid>	Name of the required BSSID of the AP.
ip-addr <ip-addr>	IP address of the AP with Wi-Fi client.

Example

The following example displays the status of the AP with Wi-Fi uplink profile. (For versions prior to ArubaOS 8.10.0.0)

```
(host) [mynode] #show ap wifi-uplink status ip-addr 10.65.43.247
WiFi uplink status
-----
SSID                gran-uplink
BSSID               ac:a3:1e:d2:19:d0
Unitcast/Multicast Encryption wpa2-aes-psk wpa2-aes-psk
Link Health (%)    20
AID                 1
Associated Time    14m:55s
Associated AP Beacon Time 10h:42m:53s
Channel            149
RSSI               52
Noise Floor        96
Phy                5GHz-VHT-20sgi-3ss
Maximum Speed (mbps) 288
Overall/Tx/Rx Goodput (mbps) 17.7 17 23.7
Last Tx Timestamp  2019-02-28 15:43:29
Last Rx Timestamp  2019-02-28 15:43:29
Last Tx Rate (mbps) 6
Last Rx Rate (mbps) 173
Last ACK RSSI      52
```

The following example displays the status of a Wi-Fi 6E AP with Wi-Fi uplink profile on a 6 GHz band (ArubaOS 8.10.0.0 or later versions).

```
(host) [mynode] #show ap wifi-uplink status ap-name ap655-8391
WiFi uplink status
-----
SSID                               test-wifi-wpa3
BSSID                               1c:28:af:68:2a:70
Unicast/Multicast Encryption       wpa3-sae-aes wpa3-sae-aes
Link Health (%)                     100
AID                                 16
Associated Time                     14m:47s
Associated AP Beacon Time           2d:13h:36m:10s
Channel                             37
RSSI                                68
Noise Floor                         92
Phy                                 6GHz-HE-20-2ss
Maximum Speed (mbps)               1152
Overall/Tx/Rx Goodput (mbps)       28.6 30.7 25.3
Last Tx Timestamp                   1936-08-25 14:57:28
Last Rx Timestamp                   1936-08-25 14:57:28
Last Tx Rate (mbps)                1201
Last Rx Rate (mbps)                1201
Last ACK RSSI                       51
```

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.

Command History

Command	Description
ArubaOS 8.10.0.0	The command output was modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ wpa3-sae-aes value for Unicast/Multicast Encryption parameter. ■ 6GHz value for Phy parameter.
ArubaOS 8.5.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ap wired-ap-profile

```
show ap wired-ap-profile [<profile-name>]
```

Description

Shows a list of all wired AP profiles, or displays the configuration parameters in a specific wired AP profile. If you include the optional `<profile-name>` parameter, the command will display detailed information for that one profile.

Parameter	Description
<code><profile-name></code>	Name of a wired AP profile.

Example

The output of this command shows the configuration parameters for the wired AP profile "default":

```
(host) [mynode] #show ap wired-ap-profile default
Wired AP profile "default"
-----
Parameter                               Value
-----
Wired AP enable                           Disabled
Trusted                                   not trusted
Forward mode                              tunnel
Switchport mode                          access
Access mode VLAN                          1
Trunk mode native VLAN                    1
Trunk mode allowed VLANs                  1-4094
Broadcast                                  Broadcast
```

The output of this command includes the following information:

Output	Description
Wired AP enable	Indicates whether the wired AP profile is enabled or disabled .
Forward mode	The configured forward mode for the profile: <ul style="list-style-type: none">▪ bridge: Bridge locally▪ split-tunnel: Tunnel to controller or NAT locally▪ tunnel: Tunnel to controller
Switchport mode	The profile's switching mode.

Output	Description
	<ul style="list-style-type: none"> ▪ access: Set access mode characteristics of the interface. ▪ mode: Set trunking mode of the interface. ▪ trunk: Set trunk mode characteristics of the interface.
Access mode VLAN	VLAN ID of the access mode VLAN.
Trunk mode native VLAN	VLAN ID of the native VLAN.
Trunk mode allowed VLANs	Range of allowed VLAN IDs for the native VLAN.
Trusted	Shows if the wired port on an AP using this profile is a trusted port. Possible values are Trusted or Not Trusted .
Broadcast	If set to broadcast , the wired AP port will forward broadcast traffic. If the parameter displays Do Not Broadcast , broadcast traffic will not be forwarded.

Related Commands

Command	Description
ap wired-ap-profile	This command configures a wired AP profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wired-port-profile

```
show ap wired-port-profile [<profile-name>]
```

Description

Shows all AP wired port profiles and their status.

Parameter	Description	Default
<profile-name>	Name of a wired AP profile.	default

Example

The following example shows that the controller has three wired port profiles. The **References** column lists the number of other profiles with references to the wired port profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] #show ap wired-port-profile

AP wired port profile List
-----
Name                References  Profile Status
----                -
default             3
NoAuthWiredPort    4          Predefined (editable)
shutdown            3          Predefined
Total:3
```

The following command displays information for an individual wired port profile:

```
(host) [mynode] #show ap wired-port-profile default

AP wired port profile "default"
-----
Parameter                Value
-----
Wired AP profile          default
Ethernet interface link profile default
AP LLDP profile           default
Shut down                 No
Remote-AP Backup          Enabled
AAA Profile                N/A
Time to wait for authentication to succeed 20 sec
Loop Protect Enable       Disabled
Loop Detection Interval   1
Loop Protect Auto Recovery Enable Disabled
```

Loop Protect Auto Recovery Interval	300
Storm Control Broadcast	Disabled
Storm Control Broadcast Threshold	2000

The output of this command includes the following information:

Parameter	Description
Wired AP profile	Name of a wired AP profile to be used by devices connecting the AP's wired port. The wired AP profile defines the forwarding mode and switchport values used by the port.
Ethernet interface link profile	An Ethernet Link profile to be used by devices connecting to the AP's wired port profile. This profile defines the duplex value and speed to be used by the port.
AP LLDP Profile	Name of an LLDP Profile associated with this wired port.
Shut Down?	Shows if the wired AP port is enabled (no) or disabled (yes).
Remote AP Backup	Use the rap-backup parameter to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the controller. If the AP is not connected to the controller, no firewall policies will be applied when this option is enabled. (The AAA profile will be applied when the AP is connected to controller).
AAA Profile	Name of an AAA profile to be used by devices connecting to the wired port of the AP.
Time to wait for authentication to succeed	Authentication timeout value, in seconds, for devices connecting the AP's wired port. The supported range is 1-65535 seconds, and the default value is 20 seconds.
Loop Protect Enable	Shows if loop protection is enabled or disabled.
Loop Detection Interval	Shows time in seconds after which a loop detection packet is transmitted on the AP port.
Loop Protect Auto Recovery Enable	Show if automatic recovery of the port in the AP that is shut down because of loop protection is enabled or disabled.
Loop Protect Auto Recovery Interval	Shows time in seconds after which automatic recovery of the port in the AP that is shut down because of loop protection is attempted.

Parameter	Description
Storm Control Broadcast	Shows if broadcast storm control is enabled or disabled.
Storm Control Broadcast Threshold	Shows broadcast packets per second on each Ethernet port of an AP before the Ethernet port is shut down.

Related Commands

Command	Description
ap wired-port-profile	This command configures a wired port profile.

Command History

Release	Modification
ArubaOS 8.3.0.0	Following parameters were introduced: <ul style="list-style-type: none"> ■ Loop Protect Enable ■ Loop Detection Interval ■ Loop Protect Auto Recovery Enable ■ Loop Protect Auto Recovery Interval ■ Storm Control Broadcast ■ Storm Control Broadcast Threshold
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wired stats

```
show ap wired stats {ap-name <ap-name> | ip-addr <ip-addr>} [client-ip <client-ip> | client-mac <client-mac>]
```

Description

This command shows statistics for campus and remote AP wired clients.

Parameter	Description
ap-name <ap-name>	Show wired AP statistics for a specified AP name.
ip-addr <ip-addr>	Show wired AP statistics for a specified AP by entering an IP address in dotted-decimal format.
client-ip <client-ip>	Show wired AP statistics for a specified client IP address.
client-mac <client-mac>	Show wired AP statistics for a specified client MAC address.

Example

```
(host) [mynode] # show ap wired stats ap-name rap5wn client-mac 00:14:d1:19:3c:0b
AP Wired User Statistics
-----
Counter          Value
-----
Slot              0
Port              1
VLAN              1
TX Packets        78
TX Bytes          7894
RX Packets        37
RX Bytes          5352
TX Broadcast Packets 36
TX Broadcast Bytes 4410
TX Multicast Packets 22
TX Multicast Bytes 1990
```

The output of this command includes the following information:

Output	Description
Slot	Slot number
Port	Port number

Output	Description
VLAN	Associated VLAN number
TX Packets	Number of packets sent
TX Bytes	Number of bytes sent
RX Packets	Number of packets received
RX Bytes	Number of bytes received
TX Broadcast Packets	Number of broadcast packets sent
TX Broadcast Bytes	Number of broadcast bytes sent
TX Multicast Packets	Number of multicast packets sent
TX Multicast Bytes	Number of multicast bytes sent

Related Commands

Command	Description
ap wired-ap-profile	This command configures a wired AP profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wmm-flow

```
show ap wmm-flow [ap-name <ap-name> | bssid <bssid> | dot11a | dot11g | 2.4GHZ | 5GHZ | 6GHz | essid <essid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>]
```

Description

This command shows the Wireless Multimedia (WMM) flow table.

WMM, or Wireless Multimedia Extensions, are a subset of the 802.11e standard. WMM provides for four different types of traffic classification: voice, video, best effort, and background, with voice having the highest priority and background the lowest. Issue the `show ap wmm-flow` command to view WMM flow data for all APs. Include any of the optional parameters described in the table above to filter the table by a specific AP, radio channel (a or g), or both AP and radio type.

Parameter	Description
<code>ap-name <ap-name></code>	View an AP with a specified name.
<code>bssid <bssid></code>	View data for an AP with a specific BSSID (Basic Service Set Identifier). The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP.
<code>dot11a</code> (For versions prior to ArubaOS 8.9.0.0)	Show the WMM flow table for a 802.11a radio.
<code>dot11g</code> (For versions prior to ArubaOS 8.9.0.0)	Show the WMM flow table for a 802.11g radio.
<code>2.4GHz</code> (ArubaOS 8.9.0.0 or later versions)	Show the WMM flow table for a 2.4 GHz radio.
<code>5GHz</code> (ArubaOS 8.9.0.0 or later versions)	Show the WMM flow table for a 5 GHz radio.
<code>6GHz</code> (ArubaOS 8.9.0.0 or later versions)	Show the WMM flow table for a 6 GHz radio.
<code>essid <essid></code>	View data for a specific ESSID (Extended Service Set Identifier). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
<code>ip-addr <ip-addr></code>	View an AP with a specified IP address by entering an IP address in dotted-decimal format.

Parameter	Description
ip6-addr <ip6-addr>	View an AP with a specified IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

Some examples of executing this command with various options are as follows:

```
(host) [mynode] #show ap wmm-flow ap-name ap105
(host) [mynode] #show ap wmm-flow ap-name ap105 dot11g
(host) [mynode] #show ap wmm-flow dot11a
The following example shows WMM flow data for all APs:
(host) [mynode] #show ap wmm-flow

WMM Flow Table
-----
AP Name      ESSID  Client          Description
-----
AP125-srk   NOE    00:90:7a:06:1f:5b  tsid 6:prio 6:inactivity 2157352960
us:bidir:apsd:normalack:tclas prio 6 ip DIP-192.168.101.194 DP-32514 DSCP-
48:one-match
AP125-srk   NOE    00:90:7a:06:1f:5b  tsid 0:prio 0:inactivity 100000000
us:bidir:apsd:normalack:no-match
Num Flows:0
```

The output of this command includes the following parameters:

Parameter	Description
AP name	Name of an AP with recorded WMM flows.
ESSID	Extended Service Set Identifier (ESSID) of a wireless network.
Client	MAC address of the client.
Description	<p>The description is a long string that includes the following information:</p> <p>TSID: Traffic Stream Identifier. The TSID should match the priority level for each flow.</p> <p>Priority: One of the following IEEE 802.1p priority values:</p> <ul style="list-style-type: none"> ■ 0,3 = Best Effort ■ 1,2 = Background ■ 4-5 = Video ■ 6-7 = Voice <p>Inactivity: Tspec inactivity threshold, in microseconds.</p> <p><country code>: AP country code, e.g., US.</p> <p>bidir: flow is bidirectional.</p> <p>apsd: flow has enabled auto power save delivery.</p>

Parameter	Description
	<p><ack>: Displays the ack policy negotiated for the flow. Possible values are:</p> <ul style="list-style-type: none"> ■ normalack ■ noack ■ blockack ■ resack (reserved ack) <p>Tclas: traffic classification element. Tclas information includes one of the following classification types, the 802.1p priority and IP version (version 4 or version 6)</p> <ul style="list-style-type: none"> ■ type0: Classification based on Ethernet parameters ■ type1: Classification based on TCP/UDP or IP parameters (IPv4 or IPv6) ■ type2: Classification based on based on IEEE802.1Q <p>DIP: Destination IP address for the flow.</p> <p>DP: Destination IP Port specified in the TCLAS for flow negotiation.</p> <p>DCSP: The Differentiated Services Code Point (DSCP) priority value that matches the flows 802.1p priority.</p>

Related Commands

Command	Description
wmm-dscp-mapping	This command enables or disables WMM DSCP map in the upstream direction decrypt-tunnel mode.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following parameters were introduced: (For ArubaOS 8.9.0.0 or later versions) <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz (For Wi-Fi 6E APs)
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap-crash-transfer

```
show ap-crash-transfer
```

Description

This command displays info for the AP crash transfer feature, which transfers AP coredump files to the controller flash memory if no dumpserver is configured.

The command `ap system-profile <profile> dump-server <server>` specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the `ap-crash-transfer` command to save dump files to the controller flash memory.



If you define a dump server and issue the `ap-crash-server` command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)[mynode] #show ap-crash-transfer
AP Crash Transfer:enabled
AP Crash folder limit:50 MB (non-editable)
```

Related Commands

Command	Description
<code>ap-crash-transfer</code>	This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Mode
All platforms	Base operating system.	Enable or config mode on managed devices.

show ap zigbee-client-database

show ap zigbee-client-database

Description

This command shows all AP's Zigbee client information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show arp

```
show arp
  counters
  vlan <vlanid>
```

Description

This command shows Address Resolution Protocol (ARP) entries for the controller.

Parameter	Description
counters	Shows ARP information on ARP counters.
vlan <vlanid>	Shows ARP information for a VLAN Interface Number. 1–4094

Example

```
This example shows configured static ARP entries for the controller.
(host) [mynode] #show arp
Protocol      Address      Hardware Address      Interface
Internet     10.3.129.98  00:1A:1E:C0:80:28    vlan1
Internet     10.3.129.253 00:0B:86:42:35:80    vlan1
Internet     10.3.129.250 00:1A:92:45:DB:00    vlan1
Internet     10.3.129.99  00:1A:1E:C0:1C:60    vlan65
Internet     10.3.129.96  00:1A:1E:C0:80:1E    vlan65
Internet     10.3.129.254 00:0B:86:02:EE:00    vlan1
```

The output of this command includes the following parameters:

Parameter	Description
Protocol	Protocol using ARP. Although the controller will most often use ARP to translate IP addresses to Ethernet MAC addresses, ARP may also be used for other protocols, such as Token Ring, FDDI, or IEEE 802.11, and for IP over ATM.
Address	IP address of the device.
Hardware Address	MAC address of the device.
Interface	Interface used to send ARP requests and replies.

Related Commands

Command	Description
arp	This command adds a static Address Resolution Protocol (ARP) entry.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show audit-trail

```
show audit-trail [history | login <number>| <number>]
```

Description

Shows the controller's audit trail log.

Parameter	Description
history	Shows audit trail history log.
login <number>	Starts displaying the log output from the specified number of lines from the end of the login or logout log. 1-65535
<number>	Starts displaying the log output from the specified number of lines from the end of the log. 1-65535

Example

By default, the audit trail feature is enabled for all commands in configuration mode. The example below shows the most recent ten audit log entries for the managed device.

```
(host) [mynode] #show audit-trail 10
Feb  5 06:13:17 cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:20:13 cli[1239]: USER: admin connected from 10.240.16.118 has
logged out.
Feb  5 06:24:37 cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:37:01 cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap
"mp-only" no vap-enable > -- command executed successfully
Feb  5 06:37:14 cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap
"mp-a-only" no vap-enable > -- command executed successfully
Feb  5 06:37:20 cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap
"default" no vap-enable > -- command executed successfully
Feb  5 06:37:29 cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap
"mpp-a-only" no vap-enable > -- command executed successfully
Feb  5 06:46:10 cli[1239]: USER:admin@10.3.129.250 COMMAND:<interface
gigabitethernet "1/2" port monitor igigabitethernet "1/1" > -- command
executed successfully
Feb  5 06:57:44 cli[1239]: USER:admin@10.3.129.250 COMMAND:<ap system-
profile "default" heartbeat-dscp 12 > -- command executed successfully
Feb  5 07:05:48 cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap
"mp-a-only" vap-enable > -- command executed successfully
```

The example below displays international characters added in the ESSID, in unicode format.

```
(host) [mynode] #show audit-trail 3
Jun 7 00:30:51 profmgr[5755]: USER:admin@10.1.4.102 NODE:"/md"
COMMAND:<wlan ssid-profile chineseSSIDProfile> -- command executed
successfully
Jun 7 00:31:36 profmgr[5755]: USER:admin@10.1.4.102 NODE:"/md"
COMMAND:<wlan ssid-profile chineseSSIDProfile> -- command executed
successfully
Jun 7 00:31:36 profmgr[5755]: USER:admin@10.1.4.102 NODE:"/md"
COMMAND:<wlan ssid-profile chineseSSIDProfile essid
\u4e2d\u6587\u65e0\u7ebf\u7f51> -- command executed successfully
```

Related Commands

Command	Description
audit-trail	Enable or disable the audit trail feature using the command.

Command History

Release	Modification
ArubaOS 8.4.0.0	The output displayed international characters in the ESSID, in unicode format.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show auth-tracebuf

```
show auth-tracebuf [count <1-250> | [failures] | mac <address>]
```

Description

This command shows the trace buffer for authentication events. Use the output of this command to troubleshoot 802.1X authentication errors. Include the <address> parameter to filter data by the MAC address of the client which is experiencing errors.

Parameter	Description
count <number>	Limits the output of the command to the specified number of packets. 1-250
failures	Filters the output of this command to display only authentication failures
mac <address>	Filters the output of this command to display only information for a specified MAC address.

Example

The example below shows the most recent ten trace buffer entries for the controller. Each row includes the following information:

```
(host) [mynode] # show auth-tracebuf count 10
Auth Trace Buffer
-----
Feb  5 08:08:29 wpa2-key2          -> 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:30 wpa2-key1          <- 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:30 wpa2-key2          -> 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:31 wpa2-key1          <- 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:31 station-down      * 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - -
Feb  5 08:08:31 station-up        * 00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - - wpa2 psk aes
Feb  5 08:08:31 station-data-ready * 00:09:ef:05:1e:b2
00:00:00:00:00:00 66 -
```

```

Feb  5 08:08:31 wpa2-key1          <-  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:31 wpa2-key2          ->  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:32 wpa2-key1          <-  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:32 wpa2-key2          ->  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:33 wpa2-key1          <-  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:33 wpa2-key2          ->  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:34 wpa2-key1          <-  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:34 wpa2-key2          ->  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 119 mic failure
Feb  5 08:08:35 wpa2-key1          <-  00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - 117
Feb  5 08:08:35 station-down      *   00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - -
Feb  5 08:08:35 station-up        *   00:09:ef:05:1e:b2
00:1a:1e:97:e5:42 - - wpa2 psk aes
Feb  5 08:08:35 station-data-ready *   00:09:ef:05:1e:b2
00:00:00:00:00:00 66 -

```

Each row in the output of this table may include some or all of the following information:

- A timestamp that indicates when the entry was created
- The type of exchange that was made
- The direction the packet was sent
- The source MAC address
- The destination MAC address
- BSSID/Server Name
- The packet number
- The packet length
- Additional information (if available); for example, username, encryption and WPA type, or reason for failure

Related Commands

Command	Description
aaa auth-trace	This command sets parameters for debug tracing in AUTH (light weight tracing).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show banner

```
show banner
show bannervia
```

Description

This command shows the current login banner. Use this command to review the banner message that appears when you first log in to the controller's command-line or browser interfaces.

Parameter	Description
banner	Displays the Message of the Day banner.
bannervia	Displays the VIA login banner message.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host) [mynode]# show banner
This testlab controller is scheduled for maintenance starting Saturday night at
11 p.m.
```

Related Commands

Command	Description
banner	Configures a banner message.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on Mobility Conductor and managed devices.

show ble_relay

```
show ble_relay
  apbinfo_ack_state
  azure-iothub-log
  disp-attr
  iot-profile
  iotRequests
  jobs
  papi-stats
  report
  tag-report
  transport_context
  ws-log
```

Description

This command displays all the values configured for Bluetooth Low Energy (BLE) relay on devices.

Parameter	Description
apbinfo_ack_state	Display APB acknowledgment information.
azure-iothub-log	Display Azure IoT Hub connection logs.
disp-attr	Display value of attribute
iot-profile	Display recent iot profile and transport context
iotRequests	Show JSON blobs received thru REST API calls as part of IoT gateway functionality
jobs	Show ble relay job queue status
papi-stats	Display PAPI stats for ble_relay.
report	Show logs for most recent beacon update
tag-report	Display recent tag data sent via websocket
transport_context	Display transport context information.
ws-log	Show web socket connection logs

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay apbinfo_ack_state

```
show ble_relay apbinfo_ack_state
```

Description

This command displays APB acknowledgement information for Bluetooth Low Energy (BLE) relay on devices.

Example

The following example displays the BLE relay APB information:

```
(host) [mynode] #show ble_relay apbinfo_ack_state

BLE Relay APBInfo Ack Debug Information
-----
AP          Eth MAC          TimeAcked          Profile 0  Profile 0 State
Profile 1  Profile 1 State  Profile 2  Profile 2 State  Profile 3  Profile
3 Statte
--          -
-----
-----
-----
wli-555    bc:9f:e4:ca:b1:ad  2000-03-05  03:34:17  --          --
--          --          --          --          --          --
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay disp-attr

```
show ble relay disp-attr all
```

Description

This command shows the BLE relay attributes.

Parameter	Description
all	Displays all the attributes.

Example

The following example displays the BLE relay attributes:

```
(host) [mynode] #show ble_relay disp-attr all
=====
WebSocket Connect Request      : Yes
Tag Logging                    : Off
LogLevel                       : 31
Note: Loglevel List: Error (0x1), Warn (0x2), Notice (0x4), Info (0x8),
Debug (0x10), Parser (0x20), Header (0x40), Ext (0x80), Client (0x100),
Latency (0x200).
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.
ble_relay set-attr	This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay iot-profile

```
show ble relay iot-profile
```

Description

This command shows the BLE relay IoT profile details.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The command displays the BLE relay IoT profile details.

```
# show ap debug ble-relay iot-profile
ConfigID                               : 7
-----Profile [mbm]-----
Identifier                               : 1639551961
serverURL                               :
https://edit.meridianapps.com/api/beacons/manage
serverType                               : Meridian Beacon Management
deviceClassFilter                       : Aruba Beacons
reportingInterval                       : 600 second
authentication-mode                     : none
accessToken                             :
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzIjo1NjQwNzcyODI5MzE1MDcyLCJ0IjoxNjM
yNTE3NTg0fQ.ADhJA8hGnhiT-c0pds4t7rw6P71S22bXherecEk_jxE
rssiReporting                           : Average
environmentType                         : office
NOTE: An active Meridian Beacons Management profile will override the
iBeacon configuration setting on an AP's BLE radio.
Server Connection State
-----
TransportContext                       : Ready
Last Data Update                       : 2021-12-15 07:06:44
Last Send Time                         : 2021-12-15 07:06:44
Last Receive Time                      : 2021-12-15 07:06:44
TransType                              : Https
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command	Description
ble_relay set-attr	This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay iotrequests

show ble relay iotrequests

Description

This command shows JSON blobs received through REST API.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay jobs

```
show ble relay jobs
```

Description

This command shows the Bluetooth Low Energy (BLE) relay job queue status.

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.
ble_relay set-attr	This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay papi-stats

```
show ble_relay papi stats
```

Description

This command displays PAPI statistics for Bluetooth Low Energy (BLE) relay on devices.

Example

The following example displays the BLE relay PAPI statistics:

```
(host) [mynode] #show ble_relay papi-stats
```

```
BLE Relay PAPI Stats
```

```
-----  
Current system time: 03:41:44
```

```
Counters
```

```
-----  
Message Topic      Inbound  Outbound  
-----  
bmrequest          0        0  
bmresponse         0        0  
asset-track        0        0  
amon               0        0  
ath                0        0  
atw                0        0  
iotops             0        0  
atw-token          0        0  
apb-info           38523    0  
apb-info-ack       0        41619  
iot-cfg            0        9571  
sb-api-southbound 0        0  
sb-api-northbound 0        0
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay report

show ble_relay report

Description

This command shows logs for the most recent beacon update.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay tag-report

```
show ble relay tag-report <profile-name>
```

Description

This command shows the BLE relay tag data.

Parameter	Description
<profile-name>	Name of the IoT profile.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.
ble_relay set-attr	This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay transport_context

```
show ble_relay transport_context
```

Description

This command displays transport context information for Bluetooth Low Energy (BLE) relay on devices.

Example

The following example displays the transport context information:

```
(host) [mynode] #show ble_relay transport_context

BLE Relay Transport Context Debug Information
-----
Index  ServerType  State  Flag  PendingDelete  ConfigPtr  ConfigName
ConfigIndex
      x
-----
-----
-
0      --      --      --      --      --      --
1      --      --      --      --      --      --
2      --      --      --      --      --      --
3      --      --      --      --      --      --
4      --      --      --      --      --      --
5      --      --      --      --      --      --
6      --      --      --      --      --      --
7      --      --      --      --      --      --
8      --      --      --      --      --      --
9      --      --      --      --      --      --
```

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble_relay ws-log

```
show ble relay ws-log <profile-name>
```

Description

This command shows the BLE relay work queue session logs of each IoT transport profile.

Parameter	Description
<profile-name>	Name of the IoT profile.

Related Commands

Command	Description
ble_relay	This command configures the Bluetooth Low Energy (BLE) relay on devices.
ble_relay set-attr	This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show ble service-profile

show ble service-profile <profile-name>

Description

This command displays the Bluetooth Low Energy (BLE) service profiles.

Parameter	Description
<profile-name>	Displays the BLE service profile specified by the name.

Example

The following command exports the AP's BLE iBeacon information into a CSV file:

```
(host) [mynode] #show ble service-profile default

Ble Service Profile "default"
-----
Parameter          Value
-----
Advertisement Format  ibeacon
Radio Instance      all
Include Ap Group    lobby
Major Range         0-65535
Minor Range         0-65535
uuid                4152554E-F99B-4A3B-86D0-947070693A78
```

Related Commands

Command	Description
ble service-profile	Configures the BLE service profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show block-redirect-url

block-redirect-url <string>

Description

This command show redirect URL for blocked content.

Example

Execute the following command to display the redirect URL for blocked content.

```
(host) [mynode] (config) #show block-redirect url  
  
Redirect URL for blocked web content  
-----  
Name          URL  
----          -  
Redirect URL
```

Related Command

Command	Description
block-redirect-url	Defines the redirect URL for blocked content.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show bocmgr

```
show bocmgr instance
  instance {device <device-id>}{interface tunnel|vlan {intf-id
<intfid>}|<nodepath>} {pool dhcp|tunnel|vlan {pool-name <pool-name>}|<nodepath>}
  pool {dhcp|intf|tunnel|vlan {pool-name <pool-name>}|<nodepath>}|{intf tunnel|vlan
{intf-id <intfid>}|<nodepath>}
```

Description

This command shows details about dynamic VLAN, tunnel, and DHCP pools.

Parameter	Description
device <device-id>	Show pools information for a device with the specified MAC address (device ID).
interface tunnel vlan	Show pool information for a specific tunnel or vlan
intf-id <intfid>	Show pool information for the specified tunnel or interface ID
<nodepath>	Show pool information for a configuration node at the specified path. (For example, /md/west/sunnyvale.)
pool dhcp tunnel vlan	Show pool information for the specified pool type.
pool-name <pool-name>	Show a list of devices using the specified pool.
<nodepath>	Show pool information for a configuration node at the specified path. (For example, /md/west/sunnyvale.)
pool dhcp {[intf]tunnel vlan}	Show pool information for the specified interface or pool type.
pool-name <pool-name>	Show details about a pool with the specified pool name
intf-id <intfid>	Display pool details info for the specified tunnel or interface ID
<nodepath>	Display pool details info for a configuration node at the specified path. (For example, /md/west/sunnyvale.)

Example

The following command shows the DHCP pool used by the configuration /md/east.

```
(host) [md])#show bocmgr instance pool dhcp /md/east
DHCP Instance(s)
-----
```

Device Name	Pool Name	Net	Mask	Vlan Id	Vlan IP
00:0b:86:99:88:17	testpool	4.1.0.0	255.255.255.192	2	4.1.0.1
00:0c:29:0e:56:65	testpool	4.1.0.64	255.255.255.192	2	4.1.0.65
00:0b:86:be:81:30 4.1.0.129	testpool	4.1.0.128	255.255.255.192	2	

Related Command

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.
ip dhcp pool	Use this command to configure DHCP.
ip tunnel pool	Use this command to configure tunnel.
ip vlan pool	Use this command to configure VLAN pools.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on the Mobility Conductor.

show boot

show boot [history]

Description

Displays the boot parameters, including the boot partition and the configuration file used when booting the controller.

Parameter	Description
history	Displays the controller's reloads and upgrade history.
upgrade-history	Display image upgrade history parameters.

Example

```
(host) [mynode] #show boot history
Reboot History Table
-----
No  Description                                     User  Role
  Timestamp
--  -----
----
1  Upgrade Failed:while downloading image:ArubaOS_SC_8.0.0.0-svcs-ctrl_
54589  admin    root  10.20.104.237  Thu Apr 14 21:57:01 2016
2  Upgrade to ArubaOS_SC_8.0.0.0-svcs-ctrl_54589 on partition 1 Successful.
    admin    root  10.20.104.237  Thu Apr 14 22:07:39 2016
3  Controller Reboot initiated.
    admin    root  10.20.104.237  Thu Apr 14 22:08:01 2016
4  Reboot Cause: User reboot.
    user     root  10.11.8.227   Thu Apr 14 22:09:45 2016
```

Related Commands

Command	Description
boot	Configures boot parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show branch-gateway-peer

show branch-gateway-peer

Description

This command shows Branch Gateway peer information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command shows Branch Gateway peer information:

```
(host)[mynode] #show branch-gateway-peer
IP Address of Transit VLAN in Peer: 0.0.0.0
Transit VLAN Interface: N/A
```

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on the Mobility Conductor.

show branch-uplink-pool

show branch-uplink-pool

Description

This command shows branch uplink pool configured for branch deployment, if uplink IPs conflict. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the Mobility Conductor.

show bulkedit

```
show bulkedit {headers | status}
```

Description

This command shows the bulkedit information such as the list of supported bulkedit headers or the status of the last bulkedit transaction.

Parameter	Description
headers	Show list of supported bulkedit headers.
status	Show status of last bulkedit transaction.

Example

The following are examples of executing the `show bulkedit` command:

```
(host) [mynode] #show bulkedit headers
(host) [mynode] #show bulkedit status
```

Related Commands

Command	Description
bulkedit import csv	Use the <code>bulkedit import csv</code> command to import data from a <code>.csv</code> file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on the managed device or the Mobility Conductor.

show ca-bundle version

```
show ca-bundle version
```

Description

This command displays the version number of CA certificates.

Example

The following command displays the version number of CA certificates:

```
(host) [mynode] #show ca-bundle version
Active CA Bundle version: 1
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on managed devices.

show ccm-debug memory-usage

```
show ccm-debug memory-usage {non-profile | profile}
```

Description

This command shows the memory usage information.

Parameter	Description
non-profile	Shows memory usage - non-profile command.
profile	Shows memory usage - profile command.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ccm-debug memory-usage non-profile  
  
NON-PROFILE Memory Usage Summary:  
  
Memory used for commandobj storage:: 6562  
Memory used by buffer management:: 0  
Memory Usage Total:: 6562
```

Related Commands

Command	Description
ccm-debug	<ul style="list-style-type: none">▪ ccm-debug config-rollback—Rolls back the configuration of a node to the previous version.▪ ccm-debug full config sync—Request a full configuration sync.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on the managed device or the Mobility Conductor.

show clock

```
show clock [cli-timestamp|timezone]
```

Description

This command shows the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled. Include the optional summer-time parameter to display configured daylight savings time settings. The timezone parameter shows the current timezone, with its time offset from Greenwich Mean Time.

Parameter	Description
cli-timestamp	Shows if clock cli-timestamp is enabled or disabled.
summer-time	Shows summer (daylight savings) time settings.
timezone	Show the configured timezone for the managed device.

Example

The output below shows the current zone time on the managed device clock.

```
(host) [mynode] #show clock timezone
clock timezone PST -8
```

Related Commands

Command	Description
clock summer-time recurring	Configures daylight savings /summer time settings
clock timezone	Configures the timezone for the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show cluster-config

show cluster-config

Description

This command show the cluster configuration for the control plane security feature.

When you issue this command from the cluster *root*, the output of this command shows the cluster role of the managed device, and the IP address of each member node in the cluster.

When you issue this command from a cluster *member*, the output of this command shows the cluster role of the managed device, and the IP address of the cluster root.

Example

In the example below, the **Cluster Role** section in the output of this command shows that the managed device on which the command was issued is the cluster root. The **Cluster IPSEC controllers** section of the output shows the IP address of each cluster member.

```
(host) [mynode] (config) #show cluster-config

Cluster Role
-----
Root
----

Cluster IPSEC controllers
-----
Switch IP address of Cluster-Members  Key
-----
172.21.18.18      *****
172.21.18.19      *****
```

Related Commands

Command	Description
control-plane-security	Configures the control plane security profile.
cluster-member-ip	Sets the controller as a control plane security cluster root, and specifies the IPsec key for a cluster member.
cluster-root-ip	Sets the controller as a control plane security cluster member, and defines the IPsec key for communication between the cluster member and the controller's cluster root.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on cluster member or cluster root controllers.

show cluster-switches

show cluster-switches

Description

Execute this command on a Mobility Conductor using control plane security in a multi-master/ conductor environment to show other managed devices to which it is connected.

When you issue this command from the cluster root, the output of this command displays the IP address of the VLAN used by the cluster member to connect to the cluster root.

When you issue this command from a cluster member, the output of this command displays the IP address of the VLAN used by the cluster root to connect to the cluster member.

Example

In the example below, the `show cluster-switches` command was issued on a cluster member. The **Switch-IP** section of the output shows the IP address of a VLAN on cluster root, indicating that the cluster member can currently communicate with the cluster root. If the managed device cannot communicate with the cluster root, this table will be blank.

```
(host) [mynode] (config) #show cluster-switches

SWITCH-IP          CLUSTER-ROLE
-----
172.21.18.18      ROOT
```

In this example, the `show cluster-switches` command was issued on a cluster root. The **Switch-IP** section of the output shows the IP address of a VLAN on each cluster member that can currently communicate with the cluster root.

```
(host) [mynode] (config) #show cluster-switches

SWITCH-IP          CLUSTER-ROLE
-----
172.21.18.18      MEMBER
172.21.18.19      MEMBER
```

Related Commands

Command	Description
control-plane-security	Configures the control plane security profile.

Command	Description
<u>cluster-member-ip</u>	Sets the controller as a control plane security cluster root, and specifies the IPsec key for a cluster member.
<u>cluster-root-ip</u>	Sets the controller as a control plane security cluster member, and defines the IPsec key for communication between the cluster member and the controller's cluster root.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show cluster-tech-support

show cluster-tech-support <filename>

Description

Displays cluster-related information in relation to the managed device.

Parameter	Description
<filename>	Specifies the file name where the command output will be stored. Maximum length of filename is 127 characters.

Example

The following command is used to store the logged cluster data:

```
show cluster-tech-support <filename>
```

Related Commands

Command	Description
show ap cluster-tech-support	This command shows cluster information of an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable on the Mobility Conductor.

show command-details

show command-details <COMMAND>

Description

This command displays the command debugging details for a command executed in the CLI session.

Parameter	Description
<COMMAND>	Enter the command that is executed in the CLI session and for which you need the command details. The command text must be within quotation marks

Example

The following example shows the output for this command.

```
(host) [mynode] #show command-details "show cellular profile"
Command Details:
-----
APP Name: Layer2/3 , Object:5126 , OperationType: Async
Objname/Container: /CHK_PARENT, MajorVer: 8 , MinorVer: 1 , Instance: NULL
Local Command: 0 , Remote Command: 0 , Remote IpAddr: NULL
Current config Node: /mm/mynode
Command Key Values:
-----
Key          Value      Instance Key
---          -
CELLULAR    CELLULAR   FALSE
PROFILE     PROFILE    FALSE
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show command-history

show command-history

Description

This command displays the command history for the CLI session. Use this command to display a list of commands that you have executed in the CLI session.

Example

The following example shows the output for this command.

```
(host) [mynode] #show command-history
CLI session history
-----
show cellular profile
show cellular profile factory
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show configuration

```
show configuration [committed <node-path> | counters platform-capability |  
datastore {[committed | default | detail | inherited | json | local | node-  
hierarchy | non-default | object | pending | stats | system | user]} | devices |  
diff | effective | failure | filtered | node-hierarchy | partial | pending |  
profile-committed | received | setup-dialog <macaddr> | similar | state | system-  
commands | unsaved-nodes]
```

Description

This command shows the saved configuration on the controller. Execute this command to view the entire configuration saved on the controller, including all profiles, ACLs, and interface settings.

Parameter	Description
committed [<node-path>]	Shows committed configuration of the configuration node.
counters platform-capability	Shows internal counters at the node and platform capability-based information.
datastore [committed default detail inherited json local node-hierarchy non-default object <objname> [detail json <node-path>] pending stats system user] [<node-path>]	Shows datastore configuration.
devices [debug <node-path>]	Shows devices list and nodes mapped to it.
diff <conf1> <conf2> [context json]	Shows the difference between two configuration items. New commands are prefixed with a plus, deleted commands are prefixed with a minus.
effective [detail <node-path>]	Shows effective configuration of devices connected to the node.
failure [all migration {[config-node device]} replace-config <A.B.C.D>]	Shows the configuration errors.

Parameter	Description
filtered	Show configuration downgraded to other versions.
node-hierarchy [debug]	Shows the configuration node hierarchy.
partial [<node-path>]	Shows incremental configuration changes between last two commits.
pending [<node-path>]	Shows pending configuration of the configuration node.
profile-committed [<node-path>]	Shows committed configuration of profiles at this node.
received	Shows the received configuration from Mobility Conductor.
setup-dialog <macaddr>	Shows the setup-dialog configuration of the device.
similar <conf1> conf2> [json]	Shows the common configuration between two configuration items.
state pending [<node-path>]	Shows the configuration state information.
system-commands {committed pending} [<node-path>]	Shows system or hidden commands at the configuration node.
unsaved-nodes	Shows the list of unsaved configuration nodes.

Example

The following example shows part of the output for this command.

```
(host) [mynode] #show configuration
version 8.0
country US
logging level warnings security subcat ids
logging level warnings security subcat ids-ap
wms
general poll-interval 60000
general poll-retries 3
```

```

general stat-update enable
general ap-ageout-interval 30
general sta-ageout-interval 30
general learn-ap disable
general persistent-known-interfering enable
!
adp discovery
adp igmp-join
adp igmp-vlan 0
.
.
.

```

Related Commands

Command	Description
configuration device	This command maps a device to an existing node in the configuration hierarchy.
configuration node	This command configures nodes in the configuration hierarchy.

Command History

Release	Modification
ArubaOS8.9.0.0	The following changes were introduced: All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.2.0.0	The following parameters were added: <ul style="list-style-type: none"> ▪ <code>filtered</code> ▪ <code>received</code> ▪ <code>setup-dialog</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on Mobility Conductor.

show controller-ip

show controller-ip

Description

Shows the IPv4 address and VLAN interface ID of the controller.

Example

The output of this command shows the IP address and VLAN interface ID.

```
(host) # show controller-ip

Switch IPv4 Address: 10.17.24.19
Switch IPv4 is configured to be Vlan Interface: 1501
Switch IPv6 Address: 2001::1
Switch IPv6 address is configured to be Vlan Interface: 1501
```

Related Commands

Command	Description
controller-ip	Sets the IP address of the to the loopback interface address or a specific VLAN interface address.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output of the command was modified to display Switch IP as Switch IPv4 .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor.

show controller-ipv6

```
show controller-ipv6
```

Description

Shows the IPv6 address and VLAN interface ID of the controller.

Example

```
(host) [mynode] # show controller-ipv6
Switch IPv6 Address: 2001::1
Switch IPv6 address is configured to be Vlan Interface: 1501
```

Related Commands

Command	Description
controller-ipv6	Sets the default IPv6 address of the to the IPv6 loopback interface address or a specific VLAN interface address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show control-plane-security

show control-plane-security

Description

Shows the current configuration of the control plane security profile. The control plane security profile enables and disables the control plane security feature and identifies campus APs to receive security certificates. Issue this command to view current control plane security settings.

Example

The following command shows whether the control plane security and auto certificate provisioning features are enabled in the control plane security profile, and the range of IP addresses that the controller will send certificates to.

```
(host)(config) #show control-plane-security
Control Plane Security Profile
-----
Parameter                               Value
-----
Control Plane Security                   Enabled
Auto Cert Provisioning                   Disabled
Auto Cert Allow All                      Enabled
Expiry timer(dd:hh)                     00:02
Auto Cert Allowed Addresses              N/A
Auto Cert Allowed IPv6 Addresses         N/A
```

Related Commands

Command	Description
control-plane-security	Configure the control plane security profile by identifying APs to receive security certificates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show country

show country [trail]

Description

Shows the country and domain upgrade trail of the controller. A controller's country code sets the regulatory domain for the radio frequencies that the APs use. This value is typically set during the controller's initial setup procedure. Use this command to determine the country code specified during setup.

Parameter	Description
trail	Displays the record showing how the switch was reconfigured for its current country domain when the controller hardware was upgraded.

Example

The output of this command shows the controller's country, model, and hardware types.

```
(host) # show country
Country:US
Model:Aruba7240-US
Hardware:Restricted US
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show cp-bwcontracts

```
show cp-bwcontract
```

Description

Displays a list of Control Processor (CP) bandwidth contracts for whitelist/allowlist ACLs.

Example

The *CP bw contracts* table lists the contract names, the ID number assigned to each contract, and its defined traffic rate in packets per second.

```
(host) #show cp-bwcontracts

CP bw contracts
-----
Contract          Id      Rate (packets/second)
-----
cpbwc-ipv4        15785   2000
cpbwc-ipv6        15798   2000
cp-rate           15809    20
```

Related Commands

Command	Description
firewall cp	This command creates a new whitelist/allowlist ACL and can associate a bandwidth contract with that ACL.
cp-bandwidth-contract	This command configures a bandwidth contract traffic rate, which can then be associated with a whitelist/allowlist session ACL.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show cp-stats

show cp-stats

Description

This command shows the control plane (CP) queue statistics.

Example

Execute the following command to view the control plane queue statistics.

```
(host) [MDC] *#show cp-stats

high vc[1]: 0x000000000108a2e0 low vc[0] = 0x0000000024540fe8
rx_sequence: 0x0034c8ee tx_sequence = 0x0034c8ee
Total Packet count at ppp xmit 0
Total Packet drop at ppp xmit interface check 0
Total Packet drop at ppp xmit 0
Total Packet count at ppp tx fixup 0
Total Packet drop at ppp tx fixup 0
ppp_rx_count@usbnet_skb_return 0
Total Packet drop at ppp xmit eth1 0
Total Packet drop at ppp proto err 0
Total Packet count at ppp_xmit_sos 0
```

Related Commands

Command	Description
control-plane-security	This command configures the control plane security profile by identifying APs to receive security certificates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show cpuload

show cpuload [current | per-cpu]

Description

The `show cpuload` command displays the controller CPU load for application and system processes. The CPU load statistics for a controller can be viewed by using the `current` parameter, or displayed per-processor by using the `per-cpu` command.

Parameter	Description
current	Include this optional parameter at the request of Aruba technical support to display additional CPU troubleshooting statistics.
per-cpu	Displays the CPU load stats for a controller by individual processor.

Example

This example shows that the majority of the controller's CPU resources are not being used by either application (user) or system processes.

```
(host)[mynode] #show cpuload
user 6.9%, system 7.7%, idle 85.4%
```

The output of this command includes the following parameters:

Parameter	Description
user	Percentage of controller CPU resources used by application processes.
system	Percentage of controller CPU resources used by system processes.
idle	Percentage of unused controller CPU resources.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show crashinfo

show crashinfo

Description

This command shows the list of crashes in the system.

Example

The following is an example for executing this command:

```
(host) [mynode] #show crashinfo
Crash Info Table
-----
Crash Time           Process Name
-----
August 18 20:43      impystart
September 08 04:18   impystart
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show crypto-local ipsec-map

```
show crypto-local ipsec [tag <ipsec-map-name>]
```

Description

Displays the current IPsec map configuration on the controller. The command `show crypto-local ipsec` displays the current IPsec configuration on the controller.

Parameter	Description
tag <ipsec-map-name>	Display a specific IPsec map.

Examples

The command `show crypto-local ipsec-map` shows the default map configuration along with any specific IPsec map configurations.

```
Crypto Map Template"ipv4mtu-standalone" 5
IKE Version: 2
IKEv2 Policy: 100
Security association lifetime seconds: 86400
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform }
Peer gateway: 10.15.141.113
Monitor IP: 0.0.0.0
Interface: VLAN 143
Source network: 3.4.5.6/255.255.255.255
Destination network: 1.2.3.4/255.255.255.255
Pre-Connect (Y/N): Y
Client NAT mode (Y/N): N
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Uplink Failover (Y/N): N
Force-Tunnel-Mode (Y/N): N
Uplink LoadBalance (Y/N): N
IP Compression (Y/N): N
DPD counters req_initd:95 req_resent:2 reply_recvd:95 peer_dead:0
DPD counters req_recvd:80 reply_sent:80
XCHG counters peer dead:0
CFG_SET Initiate Sent/Retry-NoACK/Retry-NoVLAN/Ack-Recvd= 0/0/0/0
CFG_SET Responder Recvd/Ack-sent= 0/0
Tunnel status IPSEC: UP IKE: UP
IPSEC MTU: 9216
PPK ID: 1234
```

Related Commands

Command	Description
crypto-local ipsec-map	Use this command to configure IPsec mapping for site-to-site VPN.

Command History

Release	Modification
ArubaOS 8.11.0.0	Displays the IPsec MTU value for an IPsec site-to site tunnel between two managed devices when Jumbo frames are enabled.
ArubaOS 8.10.0.0	Displays PPK ID in the IPsec map configurations on a controller.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto debug

```
show crypto debug event-logger
  count <display-max-events>
  failures
    count <display-max-events>
    mac <display-mac-addr>
  mac <display-mac-addr>
```

Descriptions

This command allows to debug crypto module.

Parameter	Description
event-logger	Enable event logging.
count <display-max-events>	Specify the number of logs to be displayed.
failures	Display failed events only.
mac <display-mac-addr>	Specify the MAC address of the device for displaying logs,

Examples

```
(host) [MDC] #show crypto debug event-logger count 5

Maximum events logged is 10000.

No      Time          Event                IP                MAC
MAP                                SPI/Cookie        Description
-----
-----
-----
1      Mar  5  04:41:19 IPSEC_TUN_UP        10.65.38.215
default-local-conductor-ipsecmap      NA                IPsec SA Up
      IKE_SAMPLE_ikeStatHdlr:3443
2      Mar  5  04:41:19 IPSEC_TUN_DOWN    10.65.38.215
default-local-conductor-ipsecmap      fc076e00         IPsec SA Down
      IPSEC_delSa:1552
3      Mar  5  04:41:04 IPSEC_TUN_UP        10.65.36.245     bc:9f:e4:ca:b1:ad
NA                                      NA                IPsec SA Up
      IKE_SAMPLE_ikeStatHdlr:3443
4      Mar  5  04:41:04 IPSEC_TUN_DOWN    10.65.36.245     bc:9f:e4:ca:b1:ad
NA                                      b23bad00         IPsec SA Down
      IPSEC_delSa:1552
5      Mar  5  04:41:04 IPSEC_REKEY_SUCCESS 10.65.36.245     bc:9f:e4:ca:b1:ad
NA                                      NA                IPsec rekey
success      childR_out:15203
```

Related Commands

Command	Description
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto dp

```
show crypto dp [peer <source-ip>]
```

Descriptions

Displays crypto data packets. Use this command to send crypto data packet information to the controller log files, or to clear a crypto ISAKMP state associated with a specific IP address.

Parameter	Description
dp	Shows crypto latest datapath packets. The output is sent to crypto logs.
peer <source-ip>	Show crypto latest datapath packets for this peer—that is, shows crypto ISAKMP state for this IP.

Examples

The command `show crypto dp` sends debug information to CRYPTO logs.

```
(host) [mynode] #show crypto dp
Datapath debug output sent to CRYPTO logs.
```

Related Commands

Command	Description
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto dynamic-map

```
show crypto dynamic-map [tag <dynamic-map-name>]
```

Descriptions

This command displays IPsec dynamic map configurations. Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can associate that map with the default global map using the command [crypto map global-map](#).

Parameter	Description
dynamic-map	IPsec dynamic map configuration.
tag <dynamic-map-name>	A specific dynamic map.

Examples

The command show crypto dynamic-map shows IPsec dynamic map configuration.

```
(host) [mynode] #show crypto dynamic-map
Crypto Map Template"default-dynamicmap" 10000
IKE Version: 1
IKEv1 Policy: All
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform, default-aes }
```

Related Commands

Command	Description
crypto dynamic-map	Use this command to configure a dynamic map.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto ipsec

```
show crypto ipsec {ipsec-map-id | mtu | sa [peer v6 <peer-ipv6> | peer <peer-ip>] | transform-set [tag <transform-set-name>]}
```

Descriptions

Displays the current IPsec configuration on the managed device. Execute the `show crypto ipsec` command to view the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security. It also displays the transform sets that define a specific encryption and authentication type.

Parameter	Description
<code>ipsec-map-id</code>	Shows IPsec MAP to ID mapping.
<code>mtu</code>	Shows IPsec max mtu.
<code>sa</code>	Shows security associations (SAs).
<code>peer ip6 <peer-ipv6></code>	Shows IPsec SAs for an IPv6 peer.
<code>peer <peer-ip></code>	Shows IPsec SAs for this IP.
<code>transform-set</code>	Shows IPsec transform sets.
<code>tag <transform-set-name></code>	Shows a specific transform set.

Examples

The `show crypto ipsec transform-set` command displays the settings for both preconfigured and manually configured transform sets.

```
(host) [mynode] #show crypto ipsec transform-set
Transform set default-transform: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-ml-transform: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-boc-bm-transform: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-cluster-transform: { esp-aes256 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-1st-ikev2-transform: { esp-aes256 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-3rd-ikev2-transform: { esp-aes128 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-gcm256: { esp-aes256-gcm esp-null-hmac }
    will negotiate = { Transport, Tunnel }
```

```

Transform set default-gcm128: { esp-aes128-gcm esp-null-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-rap-transform: { esp-aes256 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-remote-node-bm-transform: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set default-aes: { esp-aes256 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set newset: { esp-3des esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
Transform set name: { esp-aes256-gcm esp-sha-hmac }
    will negotiate = { Transport, Tunnel }

```

Use the `peer` parameter to view details about an IPsec connection.

```

(host) [mynode] #show crypto ipsec sa peer 80.254.65.210
Initiator IP: 80.254.65.210
Responder IP: 10.69.69.16
Initiator: No
Initiator cookie:018006409496dde5 Responder cookie:659f346abddccaf7
SA Creation Date: Fri Jun 25 13:21:23 2010
Life secs: 7200
Initiator Phase2 ID: 10.69.16.7/255.255.255.255
Responder Phase2 ID: 0.0.0.0/0.0.0.0
Phase2 Transform: EncAlg:esp-3des HMAC:esp-sha-hmac
Encapsulation Mode:UDP-encapsulated Tunnel
IP Compression Disabled
PFS: No
OUT SPI 1b0aa012, IN SPI 1b5c5300
Inner IP 10.69.16.7, internal type C
Aruba VIA
Reference count: 3

```

Execute the `show crypto ipsec sa` command to check the IPsec security associations.

```
(host) [mynode] #show crypto ipsec sa
```

```

IPSEC SA (V2) Active Session Information
-----
Initiator IP          Responder IP          SPI (IN/OUT)          Flags
Start Time           Inner IP
-----
-----
10.17.24.20          10.17.24.19          44e59700/2b907e00    UT2
Mar  1 20:18:09      -
Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
Total IPSEC SAs: 1

```

Related Commands

Command	Description
crypto ipsec	Use this command to configure IPsec parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto isakmp

```
show crypto isakmp
  block-aruba-ca
  cluster IPAssignPendingRaps
  clusterIP
  clusterMAC
  eap-passthrough
  groupname
  ike-mac-sa
  ipsecSPI
  key
  lc-members
  log ap <macaddr>
  packet-dump
  policy <policy-number>
  sa
  stats
  timers
  transports
  udpencap-behind-natdevice
  uplink-vlan
  vlan
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP). Use the show crypto isakmp command to view ISAKMP settings, statistics and policies.

Parameter	Description
block-aruba-ca	Shows the Configuration if Aruba-certified clients are blocked.
cluster IPAssignPendingRaps	Shows cluster configuration.
clusterIP	Show clusterIP hash table entries
clusterMAC	Show clusterMAC hash table entries
eap-passthrough	Displays configured IKEv2 EAP pass-through methods.
groupname	Shows the IKE Aggressive group name.
ike-mac-sa	Shows the MAC Hash table of IKE SA entries.
ipsecSPI	Shows IPsec SPI hash table entries.

Parameter	Description
key	Shows the IKE pre-shared keys.
lc-members	Shows cluster members.
log ap <macaddr>	Shows debugging log.
packet-dump	Shows the packet dump configuration.
policy <policy-number>	Shows the following information for predefined and manually configured IKE policies: <ul style="list-style-type: none"> ▪ IKE version ▪ encryption and hash algorithms ▪ authentication method ▪ PRF methods, ▪ DH group ▪ lifetime settings
sa	Shows the security associations.
[peer v6 <peer-ipv6> peer <peer-ip>]	Shows crypto ISAKMP security associations for this IP.
stats	Shows detailed IKE statistics. This information can be very useful for troubleshooting problems with ISAKMP.
timers	Shows IKEv1 timers.
transports	Shows IKE Transports.
udpencap-behind-natdevice	Shows the Configuration if NAT-T is enabled if managed device is behind a NAT device .
uplink-vlan	Shows the uplink vlan information .
vlan	Shows the Vlan state.

Examples

The **show crypto isakmp stats** command shows the IKE statistics.

```
(host) [mynode] #show crypto isakmp stats
Default protection suite 10001
Version 1
  encryption algorithm: 3DES - Triple Data Encryption Standard (168
bit keys)
  hash algorithm: Secure Hash Algorithm 160
  authentication method: Pre-Shared Key
```

```

Diffie-Hellman Group: #2 (1024 bit)
lifetime: [300 - 86400] seconds, no volume limit
Default RAP Certificate protection suite 10002
Version 1
encryption algorithm: AES - Advanced Encryption Standard (256 bit
keys)
hash algorithm: Secure Hash Algorithm 160
authentication method: Rivest-Shamir-Adelman Signature
Diffie-Hellman Group: #2 (1024 bit)
lifetime: [300 - 86400] seconds, no volume limit
Default RAP PSK protection suite 10003
Version 1
encryption algorithm: AES - Advanced Encryption Standard (256 bit
keys)
hash algorithm: Secure Hash Algorithm 160
authentication method: Pre-Shared Key
Diffie-Hellman Group: #2 (1024 bit)
lifetime: [300 - 86400] seconds, no volume limit

```

The **show crypto isakmp stats** command also displays the number of VIA VPN sessions initiated beyond the assigned limit:

```

(host) [mynode] (config) #show crypto isakmp stats | include max
VIA per user max session limit exceeded errors = 2

```

The **show crypto isakmp sa** command shows the IKE security associations.

```

(host) [mynode] #show crypto isakmp sa
ISAKMP SA Active Session Information
-----
Initiator IP      Responder IP      Flags              Start Time         Private IP
Peer ID
-----
-----
-----
-----
-----
10.17.61.58      10.17.61.62      i-v2-p-P Sep 16 23:59:05      -
IPV4_ADDR:10.17.61.62
Flags: i = Initiator; r = Responder
m = Main Mode; a = Agressive Mode; v2 = IKEv2; P = exchange PPK
p = Pre-shared key; c = Certificate/RSA Signature; e = ECDSA Signature
x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
3 = 3rd party AP; C = Campus AP; R = RAP; Ru = Custom Certificate RAP; I =
IAP
V = VIA; S = VIA over TCP; l = uplink load-balance
Total ISAKMP SAs: 1

```

The **show crypto isakmp sa peer** command shows crypto ISAKMP security associations for an IP.

```

(host) [mynode] #show crypto isakmp sa peer 10.30.0.2
Initiator IP: 10.30.0.1

```

```

Responder IP: 10.30.0.2
Initiator: Yes
Initiator cookie:319a7831e6be20a0 Responder cookie:0bb94aa7c77196ea
SA Creation Date: Wed Nov 10 20:35:14 2021
Life secs: 28800
Initiator Phase1 ID: C=US S=TX L=Burnet O=Aruba OU=ArubaLab CN=VMC-PPK-A
E=ken.rich@hpe.com
Responder Phase1 ID: C=US S=TX L=Burnet O=Aruba OU=ArubaLab CN=VMC-PPK-B
E=ken.rich@hpe.com
Exchange Type: IKE_SA (IKEV2)
Phase1 Transform:EncrAlg:AES256 HashAlg:HMAC_SHA2_384_192 DHGroup:20
Authentication Method: ECDSA with SHA-384 on the P-384 curve
PPK-ID: ppkid-0001
IPSEC SA Rekey Number: 0
Ipssec-map name: s2s

```

Related Commands

Command	Description
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Command History

Release	Modification
ArubaOS 8.11.0.0	The show crypto isakmp stats command displays the number of VIA VPN sessions initiated beyond the assigned limit.
ArubaOS 8.10.0.0	Shows PPK ID, if the tunnel is established using PPK exchange.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto-local isakmp

```
show crypto-local isakmp
  allow-via-subnet-routes
  ca-certificate
  certificate-group
  disable-aggressive-mode
  disable-ipcomp
  dpd
  key [peer <peer-ip> | fqdn <ike-id-fqdn>]
  max-allowed-ikev1-exchanges
  max-allowed-negotiations
  ppk
  server-certificate
  vpn-peer-passcode
  xauth
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP). Use the **show crypto-local isakmp** command to view IKE parameters.

Parameter	Description
allow-via-subnet-routes	Shows if the Mobility Conductor is configured to accept subnet routes from VIA clients.
ca-certificate	Shows all the Certificate Authority (CA) certificates associated with VPN clients.
certificate-group	Shows the existing certificate groups by server certificate name and CA certificate.
disable-aggressive-mode	Shows if aggressive-mode is enabled or disabled.
disable-ipcomp	Shows IP compression configuration.
dpd	Shows the IKE Dead Peer Detection (DPD) configuration on the managed device.
key [fqdn <ike-id-fqdn> peer <peer-ip>]	Shows the IKE pre-shared key on the managed device for site-to-site VPN. This includes keys configured by Fully Qualified Domain Name (FQDN) and local and global keys configured by IP address.
max-allowed-ikev1-exchanges	Shows the maximum allowed ikev1-exchanges allowed at a time.

Parameter	Description
max-allowed-negotiations	Shows the maximum ongoing exchanges allowed at a time. If the exchanges cross this limit, IKE_SA_INIT packets are throttled. The maximum value is set based on the platform.
ppk	Shows configured PPK IDs.
server-certificate	Shows all the IKE server certificates used to authenticate the managed device for VPN clients.
vpn-peer-passcode	Show vpn-peer passcoder.
xauth	Shows the IKE XAuth configuration for VPN clients.

Examples

The examples here show sample output for the **show crypto-local isakmp ca-certificate**, **show crypto-local isakmp certificate-group**, **show crypto-local isakmp dpd**, **show crypto-local isakmp key**, **show crypto-local isakmp ppk**, **show crypto-local isakmp server-certificate** and **show crypto-local isakmp xauth** commands:

```
(host) [mynode] #show crypto-local isakmp ca-certificate
ISAKMP CA Certificates
-----
CA certificate name  Client-VPN  # of Site-Site-Maps
-----
Aruba-Factory-CA    Y           0

(host) [mynode] #show crypto-local isakmp certificate-group

ISAKMP Certificate Groups
-----
Server certificate name  CA certificate name
-----

(host) [mynode] #show crypto-local isakmp dpd
DPD is Enabled: Idle-timeout = 22 seconds, Retry-timeout = 2 seconds, Retry-
attempts = 3

(host) [mynode] #show crypto-local isakmp key
ISAKMP Local Pre-Shared keys configured for ANY FQDN
-----
Key
---
ISAKMP Local Pre-Shared keys configured by FQDN
-----
```

```

FQDN of the host      Key
-----
servers.mycorp.com   *****

ISAKMP Local Pre-Shared keys configured by Address
-----
IP address of the host  Subnet Mask Length  Key
-----
10.4.62.10             32                   *****

ISAKMP Global Pre-Shared keys configured by Address
-----
IP address of the host  Subnet Mask Length  Key
-----
0.0.0.0                0                    *****

(host) [mynode] #show crypto-local isakmp server-certificate
ISAKMP Server Certificates
-----
Server certificate name      Client-VPN  # of Site-Site-Maps
-----
Aruba-Factory-Server-Cert-Chain  RAP-only    0

(host) [mynode] #show crypto-local isakmp xauth
IKE XAuth Enabled.

```

The example here shows the maximum allowed negotiations:

```

(host) [mynode] #show crypto-local isakmp max-allowed-negotiations
Maximum Non-SuiteB(DH-2 or DH-14, RSA certs) in-negotiations exchanges
allowed. Default: 30
Maximum SuiteB (DH-19 or DH-20, EC Certs) in-negotiations exchanges allowed.
Default: 10

```

The following CLI command displays PPK information:

```

(host) [mynode] #show crypto-local isakmp ppk
Type Flags: N = NO TPI, NH = NO TPI HEX, F = First Half, S = Second Half, T
= TPI configured
FH = First-half Hex, SH = Second-half Hex, TH = TPI Hex configured
TYPE      Peer ID      PPK ID
-----
N         PEER-ANY    demo1
N         1.1.1.1     demo2
NH        2.2.2.2     demo3
NH        2.2.2.3     demo4
T         4.4.4.4     demo5
T         4.4.4.1     demo6
TH        PEER-ANY    demo7
TH        PEER-ANY    demo8

```

```

N      5.5.5.5      demo9
T      6.6.6.6      demo10
T      7.7.7.7      demo11
N      10.17.61.62 demo12
Total PPKs configured: 12

```

Related Commands

Command	Description
crypto-local isakmp allow-via-subnet-routes	Use this command to push subnet routes to the Mobility Conductor and managed device.
crypto-local isakmp ca-certificate	Use this command to assign the Certificate Authority (CA) certificate used to authenticate VPN clients.
crypto-local isakmp certificate-group	Use this command to assign a certificate group so you can access multiple types of certificates on the same managed device.
crypto-local isakmp disable-aggressive-mode	Use this command to disable the IKEv1 aggressive mode.
crypto-local isakmp dpd	Use this command to configure IKE Dead Peer Detection (DPD) on the managed device.
crypto-local isakmp key	Use this command to configure the IKE preshared key on the managed device for site-to-site VPN.
crypto-local isakmp server-certificate	Use this command to assign the server certificate used to authenticate the managed device for VPN clients.
crypto-local isakmp xauth	Use this command to enable the IKE XAuth for VPN clients.

Command History

Release	Modification
ArubaOS 8.10.0.0	The ppk parameter was introduced.
ArubaOS 8.8.0.0	The maximum-allowed-negotiations parameter was introduced.
ArubaOS 8.0.1.0	The allow-via-subnet-routes parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show crypto-local pki

```
show crypto-local pki
  CRL
    [<name> [ALL | crlnumber | fingerprint | hash | issuer | lastupdate |
nextupdate]]
  crl-stats
  IntermediateCA
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  oosp-client-stats
  OCSPResponderCert
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  OCSPSignerCert
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  PublicCert
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  rcp [<name>]
  ServerCert
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  TrustedCA
    [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose
| serial | subject]]
  service-ocsp-responder [stats]
```

Descriptions

Execute this command to show local certificate, OCSP signer or responder certificate, and CRL data and statistics. Use the `show crypto-local pki` command to view all CRL and certificate status, OCSP client and OCSP responder status and statistics.

Parameter	Description
CRL	Shows the name, original filename, reference count and expiration status of all CRLs on this controller.
<name> ALL	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this CRL.
<name> crlnumber	Shows the number of this CRL.
<name> fingerprint	Shows the fingerprint of this CRL.
<name> hash	Shows the hash number of this CRL.

Parameter	Description
<name> issuer	Shows the issuer of this CRL.
<name> lastupdate	Shows the last update (date and time) at which the returned status is known to be correct.
<name> nextupdate	Shows the next date and time (date and time) where the responder retrieves updated status information for this certificate. If this information is not present, then the responder always holds up to date status information.
crl-stats	Shows the CRL request statistics.
IntermediateCA	Shows the name, original filename, reference count and expiration status of this certificate. NOTE: IntermediateCA has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
ocsp-client-stats	Shows the OCSP client statistics.
OCSPResponderCert	Shows the name, original filename, reference count and expiration status of all OCSPResponderCert certificates on this controller. NOTE: OCSPResponderCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
OCSPSignerCert	Shows the OCSP Signer certificate. NOTE: OCSPSignerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
PublicCert	Shows Public key information of a certificate. This certificate allows an application to identify an exact certificate. NOTE: PublicCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
rcp	Shows the revocation check point.
ServerCert	Shows Server certificate information. This certificate must contain both a public and a private key (the public and private keys must match). You can import a server certificate in either PKCS12 or X.509 PEM format; the certificate is stored in X.509 PEM DES encrypted format on the controller. NOTE: ServerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.

Parameter	Description
TrustedCA	Shows trusted CA certificate information. This certificate can be either a root CA or intermediate CA. Aruba encourages (but does not require) the signing CA of the an intermediate CA to be the controller itself.
<name> ALL	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this certificate.
<name> alias	Shows this certificate's alias, if it exists.
<name> dates	Shows the dates for which this certificate is valid.
<name> fingerprint	Shows the certificate's fingerprint.
<name> hash	Shows the hash number of this certificate.
<name> issuer	Shows the certificate issuer.
<name> modulus	Shows the modulus which is part of the public key of the certificate.
<name> purpose	Shows the certificate's purposes such as if this is an SSL server, SSL server CA and so on.
<name> serial	Shows the certificate's serial number.
<name> subject	Shows the certificate's subject identification number.
service-ocsp-responder [stats]	Shows if OCSP responder service is enabled and shows statistics.

Example

This example displays a list of all OCSP responder certificates on this controller.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert

Certificates
-----
Name                               Original Filename                Reference Count
Expired
-----
--
ocspJan28                          ocsprresp-jan28.cer              0                No
ocsprresp-standalone-feb21         ocsprresp-feb21.cer              0                No
ocsprrespFeb02                     ocsprresp-feb2.cer               1                No
OCSPResponder1                     ocsprresponder-new1.cer          0                No
ocspresponder2                     subsubCA-ocsp-res-2.cer          0                No
OCSPResponderlatest                ocsprresponder-latest.cer        0                No
```


The output of this command includes the following parameters:

Parameter	Description
Name	Name of the OCSP responder certificate.
Original Filename	Name of the original certificate when it was added to the controller.
Reference Count	Number of RCPs that reference this OCSP responder certificate, signer certificate or CRL.
Expired	Shows whether the controller has enabled or disabled client remediation with Sygate-on-demand-agent.

This example shows the dates for which this OCSP responder certificate is valid.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocsJan28 dates
notBefore=Jan 21 02:37:47 2011 GMT
notAfter=Jan 20 02:37:47 2013 GMT
```

This example displays the certificate's hash number.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocsJan28 hash
91dcb1b3
```

This example shows the purpose and information about this certificate.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocsJan28 purpose
Certificate purposes:For validation
SSL client : No
SSL client CA : No
SSL server : No
SSL server CA : No
Netscape SSL server : No
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
```

This example displays the certificate's subject.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocsJan28 subject
subject= /CN=WIN-T1BQQFMVDED.security1.qa.mycorp.com
```

Related Commands

Command	Description
crypto-local pki	This command is saved in the configuration file and verifies the presence of the certificate in the controller's internal directory structure.
crypto-local pki rcp <name>	Specifies the certificates that are used to sign OCSP responses for this revocation check point

Command History

Command	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto map

show crypto map

Descriptions

This command displays the IPsec map configurations. Use the `show crypto map` command to view configuration for global, dynamic, and default map configurations.

Parameter	Description
map	Shows the IPsec map configurations.

Examples

The output of the `show crypto map` command shows statistics for the global, dynamic, and default maps.

```
(host) [mynode] #show crypto map
Crypto Map "GLOBAL-IKEV2-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-rap-ipsecmap" 10001
IKE Version: 2
IKEv2 Policy: DEFAULT
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-gcm256, default-gcm128, default-rap-transform }
Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
IKE Version: 1
IKEv1 Policy: All
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform, default-aes }
```

Related Commands

Command	Description
crypto map global-map	Use this command to configure the default global map.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show crypto pki

```
show crypto pki csr
  CRL
  csr
  IntermediateCA
  OCSPResponderCert
  OCSPSignerCert
  PublicCert
  ServerCert
  TrustedCA
```

Descriptions

This command displays different certificates, Certificate Revocation List (CRL), and certificate signing request (CSR) for the captive portal feature.

Parameter	Description
CRL	Displays Certificate Revocation List (CRL).
csr	Displays the certificate signing request for the captive portal feature.
IntermediateCA	Displays an intermediate CA certificate
OCSPResponderCert	Displays a OCSP Responder certificate
OCSPSignerCert	Displays a OCSP Signer certificate
PublicCert	Displays a public certificate
ServerCert	Displays a server certificate
TrustedCA	Displays a trusted CA certificate

Examples

The output of the `crypto pki csr` command.

```
(host) [mynode] #show crypto pki csr

Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=US, ST=CA, L=Sunnyvale, O=sales, OU=EMEA,
    CN=www.mycompany.com/emailAddress=myname@mycompany.com
    Subject Public Key Info:
```

```

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:e6:b0:f2:95:37:d0:18:c4:ee:f7:bd:5d:96:85:
    49:a3:56:63:76:ee:99:82:fe:4b:31:6c:80:25:c4:
    ed:c7:9e:8e:5e:3e:a2:1f:90:62:b7:91:69:75:27:
    e8:29:ba:d1:76:3c:0b:14:dd:83:3a:0c:62:f2:2f:
    49:90:47:f5:2f:e6:4e:dc:c3:06:7e:d2:51:29:ec:
    52:8c:40:26:de:ae:c6:a0:21:1b:ee:46:b1:7a:9b:
    dd:0b:67:44:48:66:19:ec:c7:f4:24:bd:28:98:a2:
    c7:6b:fb:b6:8e:43:aa:c7:22:3a:b8:ec:9a:0a:50:
    c0:29:b7:84:46:70:a5:3f:09
  Exponent: 65537 (0x10001)
Attributes:
  a0:00
Signature Algorithm: sha1WithRSAEncryption
  25:ce:0f:29:91:73:e9:cd:28:85:ea:74:7c:44:ba:b7:d0:5d:
  2d:53:64:dc:ad:07:fd:ed:09:af:b7:4a:7f:14:9a:5f:c3:0a:
  8a:f8:ff:40:25:9c:f4:97:73:5b:53:cd:0e:9c:d2:63:b8:55:
  a5:bd:20:74:58:f8:70:be:b9:82:4a:d0:1e:fc:8d:71:a0:33:
  bb:9b:f9:a1:ee:d9:e8:62:e4:34:e4:f7:8b:7f:6d:3c:70:4c:
  4c:18:e0:7f:fe:8b:f2:01:a2:0f:00:49:81:f7:de:42:b9:05:
  59:7c:e4:89:ed:8f:e1:3b:50:5a:7e:91:3b:9c:09:8f:b7:6b:
  98:80
-----BEGIN CERTIFICATE REQUEST-----
MIIB1DCCAT0CAQAwZMxCzAJBgNVBAYTAlVTMQswCQYDVQIEwJDQTESMBA
GA1UEAxMRd3d3Lm15Y29tcGFueS5jb20xKDAmBgkqhkiG9w0BCQEWGXB3cmV
kZl1AYXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIG
JAoGBA0aw8pU30BjE7ve9XZaFSAWY3bumYL+SzFsgCXE7ceejl4+oh+QYre
RaXUn6Cm60XY8CxTdgzoMYvIvSZBH9S/mTtzDBn7SUSnsUoxAJt6uxqAhG+5
GsXqb3QtnREhmGezH9CS9KJiix2v7to5DqsciOrj smgpQwCm3hEZwpT8JA
gMBAAGgADANBgkqhkiG9w0BAQUFAAOBgQAlzg8pkXPpzSiF6nR8RLq30F0tU
2TcrQf97Qmvt0p/FJpfwwqK+P9AJZz013NbU80OnNJjuFWlvSB0WPhwvrmC
StAe/I1xoD07m/mh7tnoYuQ05PeLf208cExMGOB//ovyAaIPAE mB995CuQ
VZfOSJ7Y/h01BafpE7nAmPt2uYgA==
-----END CERTIFICATE REQUEST-----

```

Related Commands

Command	Description
crypto pki	Use this command to generate a certificate signing request (CSR) for the captive portal feature.
crypto pki-import	Use this command to import certificates for the captive portal feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show database

show database synchronize

Description

This command displays database synchronization status.

Parameter	Description
synchronize	Shows Multiple Master/Conductor Switches redundancy status (Master/Conductor-Master/Conductor communication).

Example

The following example displays a database synchronization status.

```
(host) [mm] (config) #show database synchronize

Last L2 synchronization time: Tue Oct 1 05:38:25 2019
Last L3 synchronization time: Tue Oct 1 04:26:09 2019
To Master/Conductor Switch at 192.168.228.4: succeeded
To Secondary Master/Conductor Switch at 2002:192:168:229::19: succeeded
WMS Database backup file size: 147035 bytes
Upgrademgr Database backup file size: 3397 bytes
Cluster upgrademgr Database backup file size: 3893 bytes
Local User Database backup file size: 37733 bytes
Global AP Database backup file size: 63738 bytes
IAP Database backup file size: 3778 bytes
Airgroup Database backup file size: 3076 bytes
License Database backup file size: 15419 bytes
CPSec Database backup file size: 3224 bytes
Bocmgr Database backup file size: 6062 bytes
Total size of Captive Portal Custom data: 0 bytes, 0 files
Total size of Captive Portal Custom data last synced: 0 bytes, 0 files
L2 Synchronization took 4 second
L3 Synchronization took 11 second
1289 L2 synchronization attempted
15 L2 synchronization have failed

10 L3 synchronization attempted
0 L3 synchronization have failed

L2 Periodic synchronization is enabled and runs every 1 minute

L3 Periodic synchronization is enabled and runs every 120 minutes
Synchronization doesn't include Captive Portal Custom data
Airmatch database gets synchronized periodically. Last synchronization time
: 20
```


Related Commands

Command	Description
<u>database synchronize</u>	This command configures the Mobility Conductor to synchronize the database with a standby or backup Mobility Conductor. This works in config mode.
<u>database-synchronize</u>	This command synchronizes the Mobility Conductor database with a standby or backup Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The output was modified to include IPv6 address of the peer Mobility Conductor in Layer-2 and Layer-3 redundancy.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show datapath

```
show datapath
  acl
    ap-name <ap-name> name <acl-name> type <acl-type>
    id <id> [verbose]
    ip-addr <ip-addr> name <acl-name> type <acl-type>
  allowed-address-list
  amsdu tx
  app-monitoring-list
  application
    [<id> | all | ap-name <ap-name> | counters | ip-addr <ip-addr> | verbose]
  bridge
    [ap-name <ap-name> | counters | ip-addr <ip-addr> | table <macaddr> |
  verbose]
  bwm
    [ap-name <ap-name> | ip-addr <ip-addr> | table | type <type-id> {[contract
  <contract-id>}]
  cluster
  compression
    [<id> | all | counters | verbose]
  cp-bwm
    [table]
  crypto
    [<id> | all | counters | verbose]
  debug
    dma [counters]
    eap [counters]
    ethlinfo
    memory
    memory-usage
    opcode
    performance [<id> | all | counters | event-guide |verbose]
    pkttrace-buffer [log {<number> | all}]
    table-limits
    tnl-stats
    trace-buffer [lines <lines>]
    trace-route
  dhcp vm-mac
  dns-cache
    [counters]
  dpdk
    mempool-stats
    ring-stats
  dpi
    app-category <appcatid>
    application <appid>
  energy-efficiency
  error counters
  esi
    [table]
  exception counters
  exthdr
  firewall-agg-sess
    [counters]
```

```
fqdn
frame
  [<id> | all | ap-name <ap-name> | counters | ip-addr <ip-addr> | slot |
  verbose]
hardware
  counters
  statistics
heartbeat stats
internal
  [dir <dir-name> file <file-name>]
ip-fragment-table
  [ipv4 | ipv6]
ip-geolocation
  [counters]
ip-mcast
  [client <client-mac> | destination | group | station]
ip-reassembly
  [counters | ipv4 | ipv6]
ip-reputation
  [counters | rtc]
ipfix statistics
ipsec-map
ipv6-mcast
  destination
  group
  station
l3-interface
lag table
maintenance
  [counters]
message-queue
  [counters]
mobility
  discovery-table
  home-agent-table
  mcast-table
  stats
nat
  [ap-name <ap-name> | ip-addr <ip-addr> | table]
netdest-id
  ap-name <ap-name>
  ip-addr <ip-addr>
  <id>
network
  egress
  ingress
nexthop-list [ipv4 | ipv6]
openflow
  acl
  acl-action-table
  auxiliary
  session [<A.B.C.D>]
  statistics
outstanding-buffers
papi [counters | remote-device-table {counters | ipv6}]
port
```

```

    [ap-name <ap-name> [table] | ip-addr <ip-addr> [table] | untrusted-vlan
    <slot/module/port> | vlan-table <slot/module/port>]
qat
rap-bw-resv
    ap-name <ap-name> [advanced]
    ip-addr <ip-addr> [advanced]
rap-pkt-trace
    ap-name <ap-name>
    ip-addr <ip-addr>
rap-stats
    ap-name <ap-name>
    ip-addr <ip-addr>
remote-user table
    ipv4
    ipv6
role-cp-table
route
    [ap-name <ap-name> | counters | ip-addr <ip-addr> | ipv4 | ipv6 | table |
    verbose]
route-cache
    [ap-name <ap-name> | counters | ip-addr <ip-addr> | ipv4 | ipv6 | table |
    verbose]
scheduler
    interface <slot/module/port>
    table
services
session
    [ap-name <ap-name> |
    counters |
    dhcp-perf |
    dpi [counters [all | top | uplink-vlan <uplinkvlan>] | table [<A.B.C.D> |
    appid <app-id>]] |
    high-value [user <macaddr>] |
    ip-addr <ip-addr> |
    ip-classification |
    ipv6 [counters | dhcp-perf | dpi [counters [top]] | high-value | perf | {table
    [<X:X:X:X::X> | appid <app-id>]} | verbose | web-cc [counters | dpi]] |
    perf |
    session-id <sid> [dpi] |
    table [<A.B.C.D>] |
    uplink [debug | verbose] |
    verbose |
    web-cc]
station
    [<id> | all | counters | crypto-counters | mac <macaddr> | standby | table |
    verbose]
tcp
    [app <app> | counters | tunnel table]
tunnel
    [counters | encaps | heartbeat | ipv4 | ipv6 | station-list | table | tunnel-
    id <tid> { trusted-vlan | untrusted-vlan} | verbose]
tunnel-group
uplink verbose
user
    [<id> | all | ap-name <ap-name> | counters | ip-addr <ip-addr> | ipv4 | ipv6
    | rad-counters | standby | table | verbose]

```

```

utilization
vlan
  [ap-name <ap-name> | ip-addr <ip-addr> | pvst | table]
vlan-mcast
  [ap-name <ap-name> | ip-addr <ip-addr> | table]
wan hc
  [<id> | all | counters | verbose]
web-cc
  [counters]
wifi-reassembly
  [<id> | all | counters | verbose]
wmm
  [counters]

```

Description

Displays system statistics for the managed device. Use the `show datapath` command to display various datapath statistics for debugging purposes.

MTU guidelines

- Since MTU discovery is not enforced between an AP and standby controller in a HA setup, the value of the MTU to be passed through the tunnel is not updated.
- The size of the MTU can be set to 9000, depending on the network link and AP configuration.
- In case of a heartbeat tunnel, unanswered larger frames for MTU discovery are counted as heartbeat misses.

Parameter	Description
<code>acl</code>	Displays datapath ACL entries.
<code>ap-name <ap-name></code>	Specify the name of the AP.
<code>id <id-name> [verbose]</code>	Displays datapath statistics associated with a specified ACL. The ACL index is found in the <code>show rights</code> command. The allowed range is 1-2703.
<code>ip-addr <ip-addr></code>	Specify the IP address of the AP.
<code>name <acl-name></code>	Specify the name of ACL.
<code>type <acl-type></code>	Specify the ACL Type. 0 - session-based; 1- role-based
<code>allowed-address-list</code>	Datapath allowed address list table
<code>counters</code>	Lists the number of IPv4 and IPv6 allowed addresses.

Parameter	Description
amsdu tx	Shows datapath AMSDU TX queue statistics
app-monitoring-list	Shows Airslice app monitoring list
application	Shows datapath application statistics. By default, it provides combined statistics of all CPUs.
<id>	Shows datapath application statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath application statistics for all CPUs, one by one.
ap-name <ap-name>	Specify the name of the AP.
counters	Shows application counters and errors generated by applications running on a particular AP. These include stateful firewall application layer statistics.
ip-addr <ip-addr>	Specify the IP address of the AP.
verbose	Shows datapath application statistics in detail.
bridge	Shows bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination, and flag information for an AP.
ap-name <ap-name>	Specify the name of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
counters	Shows datapath bridge table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures, and max link length.
devices	Shows datapath bridge devices.
ip-addr <ip-addr>	Specify the IP address of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
table <macaddr>	Displays the current high, maximum, and total number of bridge table entries for the Aruba controller.

Parameter	Description
verbose	Displays datapath bridge details in a tabular format.
bwm	<p>Displays the following bandwidth management table entry statistics:</p> <ul style="list-style-type: none"> ▪ Type: Indicates whether the contract is a control plane DoS contract (0), a contract configured through the bandwidth management WebUI or CLI Interfaces (1), or a contract for multicast traffic generated by the controller(2). ▪ Cont ID: An ID number unique to each contract. ▪ Rate: Contract traffic rate, in 256-byte packets per second. ▪ Policed: The number of packets dropped because the policy was applied. ▪ Avail Credits: This value is the (contract rate) per 32, and is used for internal debugging purposes. ▪ Queued Pkts/ Bytes: Number of bytes or packets currently being queued. ▪ Flags: Flags applied to the contract. ▪ CPU: A value in this column indicates that the traffic passed through the slowpath CPU, and is used for internal debugging purposes. ▪ Status: Indicates if the bandwidth contract is successfully applied.
ap-name <ap-name>	View a bandwidth contract for a specific AP.
ip-addr <ip-addr>	View a bandwidth contract for an AP with the specified IP address.
table	Displays a table of all configured bandwidth contracts.
type <type-id>	Displays only bandwidth contracts of a specific type (0,1 or 2).

Parameter	Description
<code>contract <contract-id></code>	Displays the bandwidth contracts for the specified contract id.
<code>cluster</code>	Displays datapath cluster statistics.
<code>details</code>	Displays heartbeat counters in detail with missed and delayed sequence numbers.
<code>peer <peer_ip></code>	Displays detailed cluster statistics for a specified peer.
<code>heartbeat counters</code>	Displays cluster heartbeat counters.
<code>compression</code>	Displays datapath compression statistics. By default, the combined statistics of all CPUs are shown.
<code><id></code>	Shows datapath compression statistics by specified CPU id. Valid platform CPU range may vary.
<code>all</code>	Shows datapath compression statistics for all CPUs, one by one.
<code>counters</code>	Shows datapath compression counters or statistics.
<code>verbose</code>	Shows datapath compression statistics in detail.
<code>cp-bwm</code>	Displays the data path CP bandwidth management table information.
<code>table</code>	Displays the datapath CP bandwidth management table entries.
<code>crypto</code>	Displays crypto parameter statistics including crypto, IPsec, PPTP, WEP, TKIP, AESCCM encryption and decryptions, WEP CRC, crypto hardware, XSEC, 802.1X, and L2TP information.
<code><id></code>	Shows datapath crypto statistics by specified CPU id. Valid platform CPU range may vary.
<code>all</code>	Shows datapath crypto statistics for all CPUs, one by one.

Parameter	Description
counters	Shows datapath crypto counters or statistics.
verbose	Shows datapath crypto statistics in detail.
debug	Displays datapath debug details. These are low-level datapath details.
dma [counters]	DMA statistics are displayed.
eap [counters]	EAP termination statistics are displayed.
ethlinfo	Displays IPv4 fragment table statistics.
memory	Displays SOS memory statistics.
memory-usage	Displays datapath memory used.
opcode	Displays datapath debugging information. NOTE: Use this command only under the supervision of Aruba technical support.
performance	Displays datapath debug performance statistics including the SUM or CPU, addr, and description.
<id>	Displays datapath performance counters by specified CPU ID.
all	Displays datapath debug performance for all CPUs.
counters	Displays datapath performance counters.
event-guide	Displays the following events: <ul style="list-style-type: none"> ▪ COPO ▪ L3 Cache ▪ NAE-RX ▪ NAE-TX events (by register index 0-4)

Parameter	Description
verbose	Displays debug performance statistics including: SUM or CPU, address, description, value, and difference from last show.
pktrace-buffer [log {<number> all}]	Shows the datapath packet trace buffer from log file, either as number of lines from the end or as complete packet trace log.
table-limits	Displays the datapath table upper limits.
tnl-stats [<id> all counters verbose]	Displays the Wi-Fi Tunnel Stats Exported to CP debug.
trace-buffer [lines <lines>]	Shows the datapath trace buffer, by number of lines from the end of log.
trace-route	Shows datapath route or cache tracing.
dhcp vm-mac	Shows datapath DHCP-related information; datapath VM to host client MAC mapping
dns-cache [counters]	Displays DNS cache statistics.
dppk mempool-stats ring-stats	Data Plane Development Kit. <ul style="list-style-type: none"> mempool-stats—Shows datapath DDPK memory pool statistics. ring-stats—Shows datapath DDPK ring statistics.
dpi app-category <appcatid> application <appid>	Displays the DPI application default ports. Specify the application Group ID or the application ID.
energy-efficiency	Displays the energy efficiency statistics.
error	Displays datapath error statistics or counters.
counters	Show datapath errors including SUM, CPU, Address, and description information. The output counters include, but not limited to, the following: <ul style="list-style-type: none"> BPDUs Received VOQ retries Invalid IP headers Received IKE Throttle

Parameter	Description
	<ul style="list-style-type: none"> ▪ VOQ retries ▪ Ipv4 Firewall Denied Frames ▪ Ipv6 Firewall Denied Frames ▪ IP Reassembly Failures ▪ Invalid IP headers Received ▪ Dot1Q Discards ▪ Dot1d Discards ▪ Drop cache frames ▪ AESCCM Encryption Station Not Ready ▪ AESCCM Decryption Failures ▪ AESCCM Decryption Invalid Replay Co
esi [table]	Displays the contents of the datapath ESI server table entries including server, IP, MAC, destination, VLAN, type, session and flag information.
exception counters	Displays the datapath debug exception statistics.
exthdr	Displays the datapath default IPv6 Extended Header Map.
firewall-agg-sess	Displays the datapath firewall aggregated sessions table.
counters	Displays the datapath aggregate session statistics.
fqdn	Displays datapath FQDN entries.
frame	<p>Displays frame statistics that are received and transmitted from the data path of the controller. Several output fields include the following descriptions:</p> <ul style="list-style-type: none"> ▪ Descr failures: This is the number of times a packet descriptor was not available and the packet dropped. ▪ Dot1QDiscards: The number of packets received on a trunk port where the VLAN presented did not match any configured on the controller and the packet dropped. ▪ Dot1d Discards: Spanning tree is disabled and each BPDU frame is

Parameter	Description
	<p>counted and dropped.</p> <ul style="list-style-type: none"> ▪ Denied Frames: Frames that are denied by the data path of the ACL for the controller. ▪ Spoofed MAC: Displays information about spoofed MAC frames. <p>See the Example section for a complete list of output.</p>
<id>	Displays datapath frame statistics by specified CPU ID. Valid platform CPU range may vary.
all	Displays datapath frame statistics for all cpus, one by one.
ap-name <ap-name> [counters]	Name of the AP. The <code>counters</code> parameter is optional.
counters	Displays datapath frame statistics
ip-addr <ip-addr> [counters]	IP address of the AP. The <code>counters</code> parameter is optional.
slot	Displays datapath combined frame statistics of all CPUs, including slot specific section.
verbose	Displays datapath frame statistics in detail.
hardware	Displays datapath hardware counters or hardware packet statistics information.
counters	Displays hardware counters.
statistics	Displays Hardware packet statistics.
heartbeat stats	Displays Sibyte heartbeat packet stats.
internal	Displays Internal details .
dir <dir-name>	Specify the hardware directory.
file <file-name>	Specify the file in the directory.

Parameter	Description
ip-fragment-table	Displays ip-fragment statistics including CPU, current entries, high water mark, max , total, and aged entries.
ipv4	Displays IPv4 fragment statistics.
ipv6	Displays IPv6 fragment statistics.
ip-geolocation	Datapath IP geolocation table entries.
counters	Displays IP geolocation statistics.
ip-mcast	Displays the Datapath IP Multicast Entries table statistics.
client <client-mac>	Datapath Layer 3 groups for specified client.
destination	Datapath tunnel and port membership.
group	Datapath Layer 3 groups.
station	Datapath station membership.
ip-reassembly	Displays the contents of the IP Reassembly statistics tables.
counters	IP reassembly counters.
ipv4	Displays the IPv4 contents of the IP Reassembly statistics table.
ipv6	Displays the IPv6 contents of the IP Reassembly statistics table.
ip-reputation	Datapath IP reputation table entries.
counters	Displays IP reputation statistics.
rtc	Displays IP reputation real time cache.
ipfix statistics	Displays datapath IPFIX collection statistics.
ipsec-map	Displays datapath IPsec map details.
ipv6-mcast	Displays the datapath IP multicast table statistics.

Parameter	Description
destination	Displays the IPv6 tunnel and port membership.
group	Displays the IPv6 multicast group.
station	Displays the IPv6 station membership.
l3-interface	Displays datapath Layer 3 interface table.
lag table	Displays contents of the datapath LAG or port channel table.
maintenance [counters]	Displays datapath maintenance statistics.
message-queue [counters]	Displays statistics of messages received by a CPU from other datapath CPUs (only CPUs that receive messages and non-zero statistics are shown). The datapath SOS message queue statistics by CPU IDs and Opcode is displayed.
mobility	Displays datapath IP mobility information.
discovery-table	Displays the discovery count table that is used to keep track of per client home agent discovery.
home-agent-table	Displays the datapath HA table information.
mcast-table	Displays the mobility multicast-group table that is used to flood the multicast RA traffic to the roamed clients.
stats	Displays the statistics of the datapath mobility.
nat	Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, S1TP start, S1P end and DIP.
ap-name <ap-name> [table]	Specify the name of AP.
ip-addr <ip-addr> [table]	Specify the IP address of the AP.
table	Shows the datapath NAT table entries.

Parameter	Description
<pre>netdest-id ap-name <ap-name> ip-addr <ip-addr> <id></pre>	<p>Shows the datapath ACL netdestination table. for AP name, IP address of AP, or ID.</p>
<pre>network {egress ingress}</pre>	<p>Displays egress or ingress queue counters. The network egress output includes, but not limited to, the following fields:</p> <ul style="list-style-type: none"> ▪ CPU ▪ DP High Prio ▪ Network High Prio <p>The network ingress output includes, but not limited to, the following fields:</p> <ul style="list-style-type: none"> ▪ LIFO Queue ▪ Threshold count ▪ Empty Count ▪ Threshold Recovery ▪ Empty Recovery
<pre>nexthop-list [ipv4 ipv6]</pre>	<p>Displays information about the datapath for packets routed to next-hop devices. The output contains the following parameters:</p> <ul style="list-style-type: none"> ▪ Dest ▪ Version ▪ Nexthop ▪ Nexthop Dest ▪ Nexthop Index ▪ Nexthop Version ▪ Nexthop VLAN ▪ Nexthop Priority
<pre>openflow</pre>	<p>Displays the datapath OpenFlow information.</p>
<pre>acl</pre>	<p>Displays the datapath OpenFlow ACL table and actions.</p>
<pre>acl-action-table</pre>	<p>Displays the OpenFlow ACL action table.</p>
<pre>auxiliary</pre>	<p>Displays the datapath OpenFlow auxiliary channel information.</p>
<pre>session [<A.B.C.D>]</pre>	<p>Displays the datapath OpenFlow session table and actions. You can optionally filter the sessions based on the IP address.</p>

Parameter	Description
statistics	Displays the OpenFlow statistics in datapath.
outstanding-buffers	Displays the datapath per-station outstanding buffer statistics.
papi	Displays the datapath PAPI statistics.
counters	Displays datapath PAPI counters including: SUM or CPU, addr, description, and value.
remote-device-table [ipv6]	Displays the remote device table maintained in the datapath that contains PAPI entries for IPv6 devices.
port	Displays the datapath port table information. This includes the port number, PVID, Ingress ACL, Egress ACL, Session ACL, and the following flags: <ul style="list-style-type: none"> ▪ B: Blocked by the Spanning Tree protocol ▪ L: LSG ▪ M: Tunneled node ▪ Q: Trunk ▪ T: Trusted ▪ X: xSec ▪ Z: QinQ
ap-name <ap-name> [table]	Specify the name of the AP. Shows the datapath port table entries for the specified AP.
ip-addr <ip-addr> [table]	Specify the IP address of the AP. Shows the datapath port table entries for the specified IP.
untrusted-vlan <slot>/<module>/<port>	Shows if there are untrusted vlan entries for the indicated slot, module, and port.
vlan-table <slot>/<module>/<port>	Shows datapath port-vlan table session entries for the specified slot, module, and port.
rap-bw-resv ap-name <ap-name> [advanced] ip-addr <ip-addr> [advanced]	Displays the remote AP uplink BW reservation statistics of the Remote AP only. Specify the AP or IP address with the <i>advanced</i> parameter for Advanced Debugging Options.

Parameter	Description
<pre>rap-pkt-trace ap-name <ap-name> ip-addr <ip-addr></pre>	Specify the name of the Remote AP. Displays the remote AP packet-trace statistics of only the specified Remote AP.
<pre>rap-stats ap-name <ap-name> ip-addr <ip-addr></pre>	Specify the name of the Remote AP. Displays the remote AP statistics of only the specified Remote AP.
remote-user table	Displays the remote user table.
ipv4	Displays the IPv4 entries of the remote user table.
ipv6	Displays the IPv6 entries of the remote user table.
role-cp-table	Displays the user-role to captive-portal mapping table.
route	<p>Displays datapath route table statistics. The output of the command includes the following fields:</p> <p>Route table entries</p> <ul style="list-style-type: none"> ▪ IP ▪ Mask ▪ Gateway ▪ Cost ▪ VLAN ▪ Flags <p>IPv6 Route table entries</p> <ul style="list-style-type: none"> ▪ Prefix ▪ Gateway ▪ Cost ▪ VLAN ▪ Flags
<pre>ap-name <ap-name> [counters table verbose]</pre>	Specify the name of the AP.
counters	Displays route table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
<pre>ip-addr <ip-addr> [counters table verbose]</pre>	Specify the IP address of the AP.
ipv4	Displays datapath IPv4 routing table.

Parameter	Description
ipv6	Displays datapath IPv6 routing table.
table	Displays route table entries such as IP, mask, gateway, cost, VLAN and flags.
verbose	Displays all detailed route table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.
route-cache	Displays datapath route cache table statistics.
ap-name <ap-name> [counters table verbose]	Specify the name of the AP.
counters	Displays route cache table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
ip-addr <ip-addr> [counters table verbose]	Specify the IP address.
ipv4	Displays datapath IPv4 route cache.
ipv6	Displays datapath IPv6 route cache.
table	Displays route cache table entries such as IP, mask, gateway, cost, VLAN and flags.
verbose	Displays all detailed route cache table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.
scheduler interface <slot/module/port> table	Displays the datapath scheduler table. Specify interface for scheduler output in the slot or module or port format.
services	Displays the datapath services table statistics including protocol, port and service.
session	Displays datapath session statistics. The command output includes, but not limited to, the following fields: <ul style="list-style-type: none"> ▪ Source IP ▪ Destination IP ▪ SPort ▪ DPort ▪ Prio

Parameter	Description
	<ul style="list-style-type: none"> ▪ ToS ▪ Age ▪ Destination ▪ TAge ▪ Packets ▪ Bytes ▪ NhIdx ▪ NhIdx ▪ NhINhVer
<pre>ap-name <ap-name> [counters table [<A.B.C.D>]]</pre>	Specify the name of the AP. Counters and table are optional parameters
counters	Displays counters statistics including current entries, high water mark, maximum entries, total entries, current maximum link length, maximum link length, stale entries, aged entries, and pending delete entries.
dhcp-perf	Displays the performance details of datapath DHCP sessions.
<pre>dpi [counters [all top uplink-vlan <uplinkvlan>]]</pre>	<p>Displays Deep Packet Information for this session. The counters parameter is optional.</p> <p>The output includes, but not limited to, the following fields:</p> <ul style="list-style-type: none"> ▪ AcIVersion: This is used to store the current version number of the ACL that is used at session creation time and is used for troubleshooting purposes. ▪ PktsDpi: The number of packets sent to the DPI engine for a given session. ▪ AcIdx: The Index of the Access List entry (in a given ACL) that triggered a match during session creation. ▪ DpiTIdx: This is an index to the DPI engine Tbl and is only used for troubleshooting purposes.
high-value	Shows high- value sessions statistics.
<pre>ip-addr <ip-addr> [counters table [<A.B.C.D>]]</pre>	Specify the IP address of the AP. The counters and table parameters are optional.

Parameter	Description
ip-classification	IP reputation or geolocation information for session.
<pre> ipv6 counters dhcp-perf dpi [counters [top] high-value perf table [<X:X:X:X::X>] appid <app-id>] table <X:X:X:X::X> verbose web-cc [counters dpi] </pre>	Displays datapath IPv6 session entries and statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries and maximum link length.
perf	Displays the performance monitored for each datapath session.
session-id <sid> [dpi]	Displays datapath session FIB for a given session index. The optional <code>dpi</code> parameter displays the deep packet information for session.
table [<A.B.C.D>]	Displays all the IP flows of a wireless device or Aruba AP. Statistics include table entries including source IP, destination IP, protocol, SPort, DPort, Cntr, priority, ToS, age, destination, TAge and flags.
uplink	Displays statistics of datapath session with uplink VLAN.
verbose	<p>Displays additional information about the session that can be used by technical support for debugging purposes.</p> <p>The command output includes, but not limited to, the following additional fields:</p> <ul style="list-style-type: none"> ▪ SIDX ▪ SRTI ▪ SRCI ▪ UsrIdx ▪ UsrVer ▪ AcIVer ▪ NhIdx ▪ NhVer

Parameter	Description
web-cc	<p>Displays web-content category information about the session. The output of this command includes but not limited to the following data columns:</p> <ul style="list-style-type: none"> ▪ WebCCRep: Reputation score (integer). To see the reputation type associated with that particular score, issue the command show web-cc reputation. ▪ WebCCID: Web content category ID. To see the name of the category associated with that category ID, issue the command show web-cc category. ▪ WebCCURL: URL for that session entry.
station	Displays datapath station association table statistics.
<id>	Shows datapath station statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath station for all CPUs, one by one.
counters	Display the current and high water mark amount of 802.11 associated wireless devices on a controller. Values output from this command represent the water-marks since the last boot of the controller. This is the same value obtainable from the Num Associations output from the <code>show stm connectivity</code> command.
crypto-counters	Displays datapath station crypto counters or statistics.
mac <macaddr>	Specify the hardware address, in hexadecimal format (48-bit, station's MAC address). Shows the datapath station association with a specific MAC.
standby	Shows datapath station associated as standby.
table	Shows datapath station associations.

Parameter	Description
verbose	Shows the datapath station detail.
tcp	Displays contents of the tcp tunnel table. This command displays all TCP tunnels that are terminated by the controller.
app <app> [counters]	Specify the name of the application.
counters	Displays the TCP tunnel statistics.
tunnel table	<p>Displays the TCP tunnel table entries. This command displays the Datapath Station Table Statistics details. Display all associated wireless devices on the controller with their corresponding AP BSSID and VLAN ID. Displays the wireless device is associated with the correct encryption type (if the device is associated to an AP BSSID that has encryption enabled and verifies whether the controller is having a problem in decrypting the wireless device's frames.</p>
tcp	Displays contents of the datapath tcp table.
tunnel	<p>Displays contents of the datapath tunnel table. This command displays all the tunnels that are terminated by the controller, including the GRE tunnels of Aruba AP. For example, a GRE tunnel is created and terminated on the Aruba controller for every SSID or BSSID configured on the Aruba AP. The output of the command includes, but not limited to, the following fields:</p> <ul style="list-style-type: none"> ▪ Source ▪ Destination ▪ Port ▪ Type ▪ MTU ▪ VLAN ▪ ACLs ▪ BSSID ▪ Decaps ▪ Encaps ▪ Heartbeats ▪ Flags ▪ Encap Bytes

Parameter	Description
	<ul style="list-style-type: none"> Decap Bytes <p>NOTE: The MTU size is 9216 bytes when Jumbo frames are enabled in an IPsec site-to-site tunnel between two managed devices. The supported range has changed from 1024-1500 to 1024-9216 MTU size for an IPsec site-to-site tunnel between two managed devices when Jumbo frames are enabled.</p>
counters	Shows tunnel counters or statistics.
encaps	Shows datapath encapsulation statistics verbose.
heartbeat	Displays the datapath heartbeat tunnel details.
ipv4	Displays the TCP tunnel table filtered on IPv4 entries.
ipv6 [encaps verbose]	Displays the TCP tunnel table filtered on IPv6 entries. The encaps or verbose parameter is optional.
station-list	Displays the list of stations on the tunnel.
table	Tunnel table statistics.
tunnel-id <tid> [trusted-vlan untrusted-vlan]	Displays datapath tunnel FIB for given tunnel index. Displays the list of trusted and untrusted VLANs.
verbose	Shows datapath tunnel internal detail.
tunnel-group	Displays the tunnel group, active status and members.
user	Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.
<id>	Shows datapath user statistics by specified CPU id. Valid platform CPU range may vary.

Parameter	Description
all	Shows datapath user table for all CPUs.
ap-name <ap-name> [counters table]	Specify the name of the AP.
counters	User counters.
ip-addr <ip-addr> [counters table]	Specify the IP address of the AP.
ipv4	Displays datapath IPv4 user entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
ipv6	Displays datapath IPv6 user entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
table	User table statistics.
verbose	Shows datapath user table detail.
uplink verbose	Displays the datapath uplink table details.
utilization	Displays the current CPU utilization of datapath CPUs by CPU ID. The output of the command includes CPU ID and CPU utilization during the past 1 sec, 4 sec, and 64 sec.
vlan	Displays VLAN table information such as VLAN memberships inside the datapath including Layer 2 tunnels which tunnel L2 traffic. The output fields of the command are as follows: <ul style="list-style-type: none"> ▪ VLAN ▪ Flags ▪ Ingress RACL ▪ Ports
ap-name <ap-name> [table]	Specify the name of the AP. Shows the datapath VLAN details.
ip-addr <ip-address> [table]	Specify the IP address of the AP. Shows the datapath VLAN details

Parameter	Description
pvst	Displays the datapath VLAN table entries.
table	Displays VLAN number, flag, port and datapath VLAN multicast entries.
vlan-mcast	Displays the datapath VLAN multicast table. The output of this command displays the datapath VLAN Multicast entries for the following fields: <ul style="list-style-type: none"> ▪ VLAN ▪ Destinations
ap-name <ap-name> [table]	Specify the name of the AP. Displays the datapath VLAN multicast table for the specific AP.
ip-addr <ip-addr> [table]	Specify the IP address of the AP. Displays the datapath VLAN multicast table for the specific IP address.
table	Displays datapath VLAN Multicast table entries.
wan hc	Displays datapath WAN health check statistics. By default, combined statistics of all CPUs is shown.
<id>	Displays datapath WAN health check statistics by specified CPU ID. Valid platform CPU range may vary.
all	Displays datapath WAN health check statistics for all CPUs.
counters	Displays datapath WAN health check counters or statistics.
verbose	Displays datapath WAN health check detail.
web-cc [counters]	Displays web content classification table information. The output of this command includes but not limited to the following data columns: <ul style="list-style-type: none"> ▪ Rep ▪ ContentID ▪ TTL ▪ Age

Parameter	Description
	Include the optional <code>counters</code> parameter to display the maximum number of entries allowed in the web content category table.
<code>wifi-reassembly</code>	Displays Wi-Fi reassembly counters including CPU, current entries, high water-mark, maximum entries, total entries, and allocation failures.
<code><id></code>	Displays Wi-Fi reassembly statistics by specified CPU ID. Valid platform CPU range may vary.
<code>all</code>	Displays Wi-Fi reassembly statistics for all CPUs, one by one.
<code>counters</code>	Displays Wi-Fi reassembly counters or statistics.
<code>verbose</code>	Displays Wi-Fi reassembly detail.
<code>wmm [counters]</code>	Displays VOIP statistics, including the number of uplink and downlink resets.

Example

The following example displays information on network specific ingress-queue counters:

```

+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+
|      |      |      |      |      |      |      |      |
|      |      |      |      |      |      |      |      |
|NAE  |LIFO | Description          |Packets
|Threshold|Empty|Threshold|Empty  |
|Block|Queue|          |Received |count
|Count|Recovery |Recovery| | | |
|      |      |      |      |      |      |
|      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+
|   0|   0|ARP, HTTP (CAP), DHCP,DNS,NTP,SNMP| 61221|   0|   0|
|   0|   0|
|   0|   1|Default queue          | 432106|   0|   0|
|   0|   0|
|   0|   2|GRE (HB)              |   0|   0|   0|
|   0|   0|
|   0|   3|IP Fragments          |   0|   0|   0|
|   0|   0|
|   0|   4|SYSLOG                |   0|   0|   0|
|   0|   0|

```

```

| 0| 5|TFTP, FTP, SSH, TELNET, HTTP | 4060| 0| 0|
| 0| 0|
| 0| 6|PVST, xSTP, VRRP, LACP | 291690| 0| 0|
| 0| 0|
| 0| 7|PAPI, CFGM | 0| 0| 0|
| 0| 0|
| 0| 8|SIP, PPTP, L2TP, IKE | 134| 0| 0|
| 0| 0|
+-----+
-----+

```

The output parameters of the `show datapath network ingress` command are explained in the following table:

Output Parameter	Description
LIFO Queue	<p>The number of the queue.</p> <p>NOTE: Packets ingressing the controller toward the NAE pass through one of 9 queues. Each queue holds a maximum 1000 packets at any one time which are taken from the queue by the NAE for forwarding.</p> <p>NOTE: The number of packets that each LIFO queue can hold is platform-specific and different for each queue. For example, 780 for Default queue 1 on 7000 Series controllers and 1580 on 7200 Series controllers.</p>
Description	The type of traffic assigned to the queue.
Packets received	The aggregate number of packets received since clearing the queues or restarting the controller.
Threshold Count	The number of times the input queue is below the built-in threshold value. Threshold counts are caused by Input queue congestion where the queue is depleted below the threshold value.
Empty Count	The number of times the Input queue is empty. Empty queue counts are caused by Input queue congestion where the queue is empty without any free descriptors.
Threshold Recovery	<p>The number of times the Input queue is below the built-in threshold value, but recovered to a number above the threshold value.</p> <p>NOTE: In a stable system, the Threshold Recovery and Threshold Count will match.</p>

Output Parameter	Description
Empty Recovery	The number of times the Input queue has recovered from empty to a normal condition to a built-in low threshold. In a stable system, the Empty Recovery and Empty Count will match.

The following example displays the discovery count table that keeps track of per client home agent discovery:

```
(host) [mynode] #show datapath mobility discovery-table
Datapath Mobility Discovery Count Table
-----
Index   Valid   Version  Retry#   No-Response  Ack   Mac
  Vlan
-----
-
1       1       2        1        a             0
10:78:D2:FA:7D:38  74
The following example displays the datapath HA table information:
(host) [mynode] #show datapath mobility home-agent-table
Datapath Mobility Home Agent Table
-----
Switch IP
-----
10.16.19.14
10.16.19.140
```

The execution of the following command displays the mobility multicast-group table that floods the multicast RA traffic to the roaming clients:

```
(host) [mynode] #show datapath mobility mcast-table
```

The following example displays the statistics of the datapath mobility:

```
(host) [mynode] #show datapath mobility stats
Datapath Mobility Stats
Mcast group entry alloc errors      : 0
Frames flooded over MMG (@HA)      : 0
Frames subjected to MMG (@FA)      : 0
Frames sent to roamed clients      : 0
HA Discovery failure to notify NACK : 0
HA Discovery invalid DCT           : 0
HA Discovery DCT allocation failed  : 0
HA Discovery Probes sent           : 0
HA Discovery NULL bridge entry in DCT : 0
HA Discovery failed to start       : 0
HA Discovery successfully started   : 0
HAT insert failure                 : 0
HAT insert success                 : 0
HAT delete failure                 : 0
```

```
HAT delete success : 0
```

The following example displays the mobility multicast VLAN table information:

```
(host) [mynode] #show ip mobile multicast-vlan-table
Mobility Multicast Vlan Table
-----
Client MAC          Home vlan  Current vlan
-----
40:2C:F4:36:16:07  501       501
```

The following example displays a list of tunnels.

```
(host) [mynode] #show datapath tunnel
+-----+-----+-----+-----+
|SUM/|          |          |          |
|CPU |  Addr | Description          |          Value |
+-----+-----+-----+-----+
|  |  |  |  |  |  |
| G | [000] | Current Entries          |          10 |
| G | [002] | High Water Mark          |          12 |
| G | [003] | Maximum Entries          |        24576 |
| G | [004] | Total Entries            |          12 |
| G | [006] | Max link length          |           1 |
+-----+-----+-----+-----+
Datapath Tunnel Table Entries
-----
Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP
fragment OK
W - WEP, K - TKIP, A - AESCCM, G - AESGCM, M - no mcast src filtering
S - Single encrypt, U - Untagged, X - Tunneled node, 1(cert-id) - 802.1X
Term-PEAP
2(cert-id) - 802.1X Term-TLS, T - Trusted, L - No looping, d - Drop
Bcast/Unknown Mcast,
D - Decrypt tunnel, a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split
tunnel
V - enforce user vlan(open clients only), x - Striping IP, z - Datazone
H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t -
Cluster s-AAC tunnel
c- IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat
#          Source          Destination  Prt  Type  MTU  VLAN  AcIs
          BSSID
-----
12      SPI01972200 in  10.17.41.82  50  IPSE  1500  0  routeDest 0000
0
11      SPIFC376400out  10.17.65.115  50  IPSE  1500  0  routeDest 0001
0
Decaps      Encaps      Heartbeats  Flags          EncapKBytes  DecapKBytes
```

```

-----
6602          0          T          0          0
0            4376        T          0          0
-----

```

The following example displays output of L2 GRE Tunnel Interface.

```

(host) [mynode] #show datapath tunnel ipv6
Datapath Tunnel Table Entries
-----

Flags: E - Ether encap, I - Wi-Fi encap, R - Wired tunnel, F - IP
fragment OK
      W - WEP, K - TKIP, A - AESCCM, M - no mcast src filtering
      S - Single encrypt, U - Untagged, X - MUX, 1 - 802.1X Term
      T - Trusted, L - No looping, d - Drop Bcast/Unknown Mcast, D -
Decrypt tunnel
      a - Reduce ARP packets in the air, e - EAPOL only
      C - Prohibit new calls, P - Permanent, m - Convert multicast, n -
Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled),
      V - enforce user vlan(open clients only), z - Datazone
      H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel,
t - Cluster s-AAC tunnel
      w - Tunneler Node Heartbeat, l - Tunneler Node user tunnel
      B - Cluster A-SAC Mcast, G - Cluster S-SAC Mcast, Y - Convert BC/MC
to Unicast
#      Source          Destination          Prt  Type  MTU   VLAN  Acls
BSSID
-----
16    2046:eab::25      2047:eab::25       47   0     1280  0     0
00:00:00:00:00:00
Decaps  Encaps  Heartbeats  Flags
-----
119209  25535   28873      TEFPR

```

The following example displays the tunnel statistics.

```

(host) [mynode] #show datapath tunnel counters
+-----+
|SUM/|      |                               |                               |
|CPU | Addr | Description                    |                               | Value |
+-----+-----+-----+-----+-----+
|    | [00] | Tunnel FIB forwarded           |                               | 38437 |
|    | [02] | GRE Encap drop                 |                               | 221   |
|    | [03] | GRE Encap fallback to session |                               | 1237276789 |
|    | [04] | Tunnel FIB stale               |                               | 1176392 |
+-----+-----+-----+-----+
| G  | [00] | Current Entries                |                               | 9366  |
| G  | [02] | High Water Mark                |                               | 9703  |
| G  | [03] | Maximum Entries                |                               | 98304 |
| G  | [04] | Total Entries                  |                               | 2876603 |

```

```

| G | [06] | Max link length                7 |
| G | [07] | Current Tunnel FIB                    1 |
| G | [08] | Tunnel FIB recompute                1176170 |
+-----+-----+-----+-----+-----+-----+

```

The output parameters of the `show datapath tunnel counters` command are explained in the following table:

Output Parameter	Description
Current Entries	Number of established tunnels. A warning message is sent to the system log if the value of the <code>Current Entries</code> exceeds 80% of the <code>Maximum Entries</code> value for a controller.
Pending Deletes	Number of tunnel entries that are marked to be deleted.
High Water Mark	The maximum number of concurrently established tunnels at any given time since the last controller reboot.
Maximum Entries	Maximum number of tunnel entries that can be supported by the platform.
Total Entries	The total number of times a tunnel has been created since the last controller reboot. Only a tunnel UP event is considered. For example, if the same tunnel is created 5 times, then the total entries count increments by the value of 5.
Allocation Failures	Total number of tunnel entry allocation failures.
Max Link Length	Indicates the length of the linked list that has the maximum length in the hash table.
Current Tunnel FIB	Number of tunnel FIB entries that are recomputed and have a valid session entry and route cache entry.
Tunnel FIB Recompute	Number of invalid tunnel FIB entries for which tunnel FIB is recomputed.
Tunnel FIB forwarded	Number of packets that are forwarded through tunnel.
Tunnel FIB Egress Not Unicast	Number of packets whose bridge entry is not found or whose egress destination is not unicast.
GRE Encap drop	Number of packets that are dropped due to various reasons such as destination is not a tunnel, tunnel is not valid, packet length exceeded the allowed MTU, and so on.
GRE Encap fallback to session	Number of packets that are not permitted to be directly forwarded using tunnel FIB, but rather have to fall back to the session-route processing in the pipeline.

Output Parameter	Description
Tunnel FIB stale	Number of tunnel FIB entries that are invalid due to invalid session or tunnel version number not matching the session version number.

The following example displays a partial list of crypto parameter statistics.

```
(host) [mynode] #show datapath crypto counters
+-----+-----+-----+-----+
|SUM/|          |          |          |
|CPU |  Addr | Description                    |          |
+-----+-----+-----+-----+
|    | [000] | Crypto Requests Total          | 25751 |
|    | [002] | Crypto Response received       | 25751 |
|    | [034] | IPsec drops UDP encap NATT port mis | 60 |
|    | [153] | RSA Requests                   | 9 |
|    | [155] | RSA Response received          | 9 |
+-----+-----+-----+-----+
|    |      |          |          |
| G | [001] | Crypto Cores In Use            | 4 |
| G | [014] | DOT1X Term Buffers             | 4096 |
| G | [015] | DOT1X Term Buffers Free        | 4096 |
+-----+-----+-----+-----+
| G | [000] | Crypto Accelerator Present     | TRUE |
+-----+-----+-----+-----+
```

The following parameters appear in the output of the `show datapath crypto counters` command, and are useful for debugging purposes.

Parameter	Description
Crypto BadNPlus	Indicates a queue overrun in the output of the encryption circuit.
Crypto SendNPlusFailed	Indicates a queue overrun in the input of the encryption circuit.
IPSec Frag Failures	This counter increments when the AP detects a failure to fragment a frame before or after IPsec encryption.
IPSec Invalid Length	The inbound IPsec frame length is verified before and after decryption. If the frame length is found to be incorrect, this counter is incremented.
IKE Rate	When the managed device firewall receives a UDP packet, it determines if the packet is destined for an IKE (500) or IPsec_NATT (4500) port. This counter increments when the AP receives an initial IKE packet that has an 8-byte responder cookie defined all 0s.

The following example displays the output of the `show datapath frame` and `show datapath frame counters` commands.

```
(host) [mynode] #show datapath frame
+-----+-----+-----+-----+
|SUM/|      |      |      |      |
|CPU | Addr | Description          |      | Value |
+-----+-----+-----+-----+
|    | [00] | Allocated Frames    |      | 7068 |
|    | [01] | Max Allocated Frames|      | 7391 |
|    | [03] | Unknown Unicast    |      | 6117 |
|    | [10] | IP Reassembled Datagrams|    | 9310 |
|    | [14] | IP Reassembly Failures|    | 15791|
|    | [36] | Flood Frames       |      | 948757|
|    | [60] | VOQ retries        |      | 536  |
+-----+-----+-----+-----+
|    |      |      |      |      |
| G  | [00] | BPDUs Received     |      | 948910|
+-----+-----+-----+-----+

(host) [mynode] #show datapath frame counters
+-----+-----+-----+-----+
|SUM/|      |      |      |      |
|CPU | Addr | Description          |      | Value |
+-----+-----+-----+-----+
|    | [00] | Rx Frames          |      | 29033086|
|    | [01] | Rx Bytes           |      | 812728150|
|    | [02] | Tx Frames          |      | 3515809 |
|    | [21] | Ipv4 VPN Denied Frames|    | 6        |
|    | [27] | Ipv4 Firewall Denied Frames|    | 1        |
|    | [36] | Dot1d Discards    |      | 313     |
+-----+-----+-----+-----+
```

The following table provides description for some important output parameters of `show datapath frame` and `show datapath frame counters` commands:

Output Parameter	Description
Allocated Frames	Statically pre-allocated frames (for handling data-traffic) and dynamically allocated frames (for internal control-traffic).
Max Allocated Frames	Max watermark of Allocated Frames.
TX Underrun	Hardware counter if MAC was fetching packet data while packet is being transmitted.
TX Max Collision-Late Abort	Hardware counter if packet transmission was aborted due to maximum collision count exceeded (10 or 100 modes only) or a late abort.

Output Parameter	Description
Frame Denied L2-GRE Loop	Packets where Ingress and Egress are same (Enabled for Mobility feature only).
Unknown Unicast	Unknown dest-mac counter.
IPv6 Unknown Unicast	Unknown Unicast for IPv6 ethtype.
IP Datagrams Fragmented	IP datagrams fragmented when packet-length is greater than Tunnel MTU (Tunnel can be between controllers or controller and AP).
WIFI AMSDU	Wi-Fi A-MSDU frames received from Wi-Fi clients.
WIFI AMSDU Aggregated	A-MSDU frames sent by controller to Wi-Fi clients.
Runts Received	Packet length is less than minimum header length.
Station Not Data Ready	Packets received by a controller from the APs or Stations before they got provisioned.
Station Inactive	Packets received by a controller from the APs or Stations after they were inactive.
Association Throttle	Drops of APs or Stations Associate coming at high rate (e.g., during failover).
IKE Throttle	Drops of IKE packets coming at high rate.
IPv6 NA Spoofs	IPv6 Network Advertisement spoofs.
IPv6 NS Spoofs	IPv6 Network Solicitation spoofs.
EOP zero frames	Zero length frames.
CP Policed Frames	Packets bound to Control plane from Data plane dropped.
Seqno request failure	Wi-Fi Sequence no. request failed.
Heartbeats sent to SP	Tunnel Heartbeats punted to Slowpath (due to route-cache miss, etc.)
Heartbeats dropped by FP	Tunnel Heartbeats dropped in data plane.
POE descriptor freed	Internal counter
CP Enqueue Buffer Alloc Failure	Buffer allocation failures while sending packets to Control plane.

Output Parameter	Description
VOQ retries	Virtual Output Queues are packet exchanges between any two entities (CPU or Hardware offload engines) that have failed due to there not being any available credits. Packets are scheduled to be retried at a later point in time.
Seqno responses sent	The sequence number sent in response to sequence number requests used in Wi-Fi frames.
Dot1Q Discards	<p>The Dot1Q discard counter may increase as a result of the following:</p> <ul style="list-style-type: none"> ▪ An incoming frame's VLAN does not match a port's configured VLAN. ▪ A trunk port is not a member of the received frames's VLAN and the received frame is not an STP BPDU, CISCO BPDU or an LACP PDU. ▪ A received frame has three or more stacked (QnQ tagged) VLANs. ▪ A received frame contains more than one VLAN tag, however the expected number of VLAN tags is one. ▪ An untagged access port is not a member of the VLAN in the received frame. ▪ A station has sent a tagged VLAN frame. ▪ A received LLDP frame has no multicast destination. ▪ A received frame has no multicast destination in the VLAN group.
Dot1D Discards	<p>The Dot1d discard counter may increase as a result of the following:</p> <ul style="list-style-type: none"> ▪ If a port is in STP blocking state, then received frames are dropped. ▪ The tagged frame received on untagged port and dropped. ▪ Received frame length is less than (Ethernet + VLAN) header length. ▪ Frames that have been dropped due to bridge filtering. ▪ Port has MUX flag set but NULL egress destination. ▪ Frame drop either if destined for non-tunnel or to port channel or destination tunnel with no multicast configured. ▪ Dropped frames addressed to BPDU MACs but not configured in the bridge table. ▪ Dropped unexpected frames.

When the counter value is zero, the output parameter line is not displayed.

Some of the other output parameters that could be part of the `show datapath frame` command are as follows:

<ul style="list-style-type: none"> ■ IP Fragmentation Failures ■ IP Jumbo Fragmentation Failures ■ IP Jumbo IPSec Encryption Failures ■ IP Reassembled Datagrams ■ IP Reassembly overlaps ■ IP Reassembly PAPI Failures ■ IP Reassembly PAPI ■ IP Reassembly Failures ■ IPv6 Datagrams Fragmented ■ IPv6 Fragmentation Failures ■ IPv6 Reassembled Datagrams ■ IPv6 Reassembly overlaps ■ Invalid IP headers Received ■ Invalid IPv6 headers Received ■ Too Many IPv6 Ext. Hdrs Received 	<ul style="list-style-type: none"> ■ xSec Frames Re-Assembled ■ xSec Re-Assembly Failures ■ Flood Frames ■ Flood Frames Peak Value ■ ARP Request Spoofs ■ ARP Reply Spoofs ■ Gratuitous ARP Spoofs ■ IP spoofs ■ CPU based seqno resp ■ Frame Length Failure ■ Packet send failed and will be retried later ■ Invalid Tail Room DDMO ■ Invalid mcast entry ■ Jumbo Wi-Fi Frames ■ Invalid ingress frames ■ Invalid egress frames ■ Invalid opcode ■ Invalid Port ■ Invalid Slot ■ Invalid ACL ■ Jumbo discards 	<ul style="list-style-type: none"> ■ Jumbo recvd ■ Jumbo xmits ■ Jumbo drops ■ Jumbo wire to wireless drops ■ Jumbo xmits Failures ■ Jumbo drops [Non Jumbo Port] ■ Jumbo drops [Wireless client] ■ Flooded Jumbo Frames ■ Buffer Alloc Failure ■ NAE Transmit Failure ■ Total queued BWM packets ■ Excessive ARP Requests ■ Drops - DPI enforcement ■ Drops - WEB CC enforcement ■ IPv6 Vlan Discards ■ Drops - Wireless client garps
---	---	--

The following is an example of the `show datapath compression` command output:

```

+-----+-----+-----+-----+
|SUM/|      |      |      |      |
|CPU | Addr | Description |      | Value |
+-----+-----+-----+-----+
|    | [00] | Compression Engine Present |      | True |
|    | [01] | Comp Response received |      | 150 |
|    | [02] | Comp Response failed |      | 0 |
|    | [03] | Decomp Requests |      | 80 |
|    | [04] | Decomp Response received |      | 80 |
|    | [05] | Decomp Requests queued |      | 75 |
| G  | [06] | Compression Engine Total |      | 4 |
+-----+-----+-----+-----+

```

When the counter value is zero, the output parameter line is not displayed.

The following example displays the output of the `show datapath bwm table` command:

```

(host) [mynode] #show datapath bwm table
Datapath Bandwidth Management Table Entries
-----
Contract Types :
0 - CP Dos 1 - Configured contracts 2 - Internal contracts
-----
Flags: Q - No drop, P - No shape(Only Policed),
T - Auto tuned

```

```

-----
Rate: pps - Packets-per-second (256 byte packets), bps - Bits-per-second
-----
Cont      Avail      Queued/Pkts
Type Id    Rate      Policed    Credits    Bytes      Flags      CPU
Status
-----
0      1      9792 pps  0          305        0/0        4
ALLOCATED
0      2      3936 pps  0          123        0/0        4
ALLOCATED
0      3      65536 pps 0          2048       0/0        4
ALLOCATED
0      4      3936 pps  0          123        0/0        4
ALLOCATED
0      5      992 pps   0          31         0/0        4
ALLOCATED
0      6      992 pps   0          31         0/0        4
ALLOCATED
0      7      992 pps   0          31         0/0        4
ALLOCATED
0      8      512 pps   0          16         0/0        4
ALLOCATED
0      9      3936 pps  0          123        0/0        4
ALLOCATED
0     10      1984 pps  0          62         0/0        4
ALLOCATED
0     11      128 pps   0          4          0/0        4
ALLOCATED
1      1      20 Mbps   0          78125     0/0        6
ALLOCATED
1      2      10 Mbps   0          39063     0/0        7
ALLOCATED
1      3      5 Mbps    0          19532     0/0        5
ALLOCATED
--More-- (q) quit (u) pageup (/) search (n) repeat

```

If the policed counter is a non-zero value, it means excessive traffic of that type that has been dropped to avoid saturating the Control Plane, resulting in potential DoS.

The following table provides description for the contract IDs 1-10 as well as the corresponding firewall parameters:

Contract ID	Contract Description	Firewall Parameter
1	Rate limit Control-Plane-bound untrusted unicast packets. It is used to limit Web CC traffic to CP.	untrusted-ucast

Contract ID	Contract Description	Firewall Parameter
2	Rate limit Control-Plane-bound untrusted multicast packets. It limits ACL logging, packet capture traffic.	untrusted-mcast
3	Rate limit Control-Plane-bound trusted unicast packets.	trusted-ucast
4	Rate limit Control-Plane-bound trusted multicast packets.	trusted-mcast
5	Rate limit Control-Plane-bound routed packets.	route
6	Rate limit Control-Plane-bound GRE control-plane session mirrored packets.	sessmir
7	Rate limit Control-Plane-bound authentication-related packets.	auth
8	Rate limit Control-Plane-bound VRRP protocol packets.	vrrp
9	Rate limit Control-Plane-bound ARP protocol packets	arp-traffic
10	Rate limit Control-Plane-bound other Layer-2 or bridging packets - Non-ARP traffic.	l2-other
11	Rate limit Control-Plane-bound IP error packets.	ippkt-err

The following example displays the IPv6 route table entries of AP datapath in Spit-Tunnel forwarding mode for Remote APs:

```
(host)[mynode] #show datapath route ap-name ap303 ipv6
IPv6 Route Table Entries
-----
Flags: L - Local, P - Permanent, T - Tunnel, I - IPsec, M - Mobile, A -
ARP, D - Drop

  Prefix          Gateway          Cost  VLAN  Flags
  -----
::/0              fe80::eaf7:24ff:fe46:2ee1  0     0
2001:603::/64    2001:603::159b      0     1     L
```

The following example displays the IPv6 route cache entries of AP datapath in Spit-Tunnel forwarding mode for Remote APs:

```
(host)[mynode] #show datapath route-cache ap-name ap325 ipv6
Neighbour/Route Cache Entries
-----
```

```
Flags: L - Local, P - Permanent, T - Tunnel, I - IPsec, M - Mobile, t-
trusted, A - ARP, D - Drop, R - Route across vlan
O - Temporary, N - INactive, i - Mixed Mode IPsec
```

IP	MAC	VLAN	Flags
2001:384::250	E8:F7:24:46:2E:E1	1	
2001:603::41c	AC:A3:1E:CD:3C:F0	1	LP
2001:604::1800	00:27:10:D0:24:7C	604	
fe80::eaf7:24ff:fe46:2ee2	E8:F7:24:46:2E:E2	604	tA

The following example displays the WebCC related entries for IPv6 sessions:

```
(host)[mynode](config-submode) #show datapath session ipv6 web-cc
Datapath Session Table Entries
-----
```

Source IP	Destination IP	Prot
SPort DPort Cntr		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::2003	6
55164 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2404:6800:4003:c03::66	6
55185 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2404:6800:4003:c03::61	6
55182 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a04:4e42:2::323	6
55175 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::2005	6
55156 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::2001	6
55143 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2404:6800:4003:c03::65	6
55177 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::200a	6
55154 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2404:6800:4003:c03::54	6
55155 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:807::200e	6
55145 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:807::200e	6
55146 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::200a	6
55161 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::200a	6
55162 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::200e	6
55149 443 0/0		
2001:470:ed6c:43:181b:450a:792d:3d02	2a00:1450:400e:804::200e	6

```

55148 443 0/0
2001:470:ed6c:43:181b:450a:792d:3d02 2a00:1450:400e:804::200e 6
55151 443 0/0

```

Prio	ToS	Age	Destination	TAge	Packets	Bytes	SIDX	AclVer	Int-Flag
Sess-Flag2	-----								
0	0	5	tunnel 13	52	16	1174	91c	2092	0
0	0	4	tunnel 13	4e	26	2038	944	2092	0
0	0	4	tunnel 13	4e	44	1821	a44	2092	0
0	0	5	tunnel 13	4f	8	744	ad8	2092	0
0	0	5	tunnel 13	53	19	1360	191c	2092	0
0	0	5	tunnel 13	5b	22	2133	1a1c	2092	0
0	0	4	tunnel 13	4e	22	1544	1d44	2092	0
0	0	5	tunnel 13	58	16	1246	231c	2092	0
0	0	4	tunnel 13	53	27	2220	2344	2092	0
0	0	6	tunnel 13	5b	14	726	241c	2092	0
0	0	6	tunnel 13	5b	23	1242	271c	2092	0
0	0	5	tunnel 13	53	19	1158	281c	2092	0
0	0	5	tunnel 13	53	14	938	2b1c	2092	0
0	0	5	tunnel 13	58	580	13637	2c1c	2092	0
0	0	5	tunnel 13	58	10	818	2d1c	2092	0
0	0	5	tunnel 13	58	10	818	2e1c	2092	0

WebCCRep	WebCCId	AceIdx	Flags	CPU ID	WebCCURL

81	search-engines	(50) 451 /0	C	3	ssl.gstatic.com
92	computer/interne	(5) 451 /0	C	3	apis.google.com
92	computer/interne	(5) 451 /0	C	3	
googletagmanager.com					
10	bot-nets	(67) 451 /0	C	3	data.api.cnn.io
79	web-based-email	(55) 451 /0	C	3	gmail.com
81	computer/interne	(5) 451 /0	C	3	yt3.ggpht.com
79	computer/interne	(5) 451 /0	C	3	google-
analytics.com					
96	search-engines	(50) 451 /0	C	3	
fonts.googleapis.com					
96	internet-portals	(51) 451 /0	C	3	


```

accounts.google.com
 81      streaming-media (25 ) 451 /0   C      3      youtube.com
 81      streaming-media (25 ) 451 /0   C      3      youtube.com
 96      search-engines  (50 ) 451 /0   C      3
fonts.googleapis.com
 88      computer/interne(5  ) 451 /0   C      3
ajax.googleapis.com
 50      content-delivery(65 ) 451 /0   C      3      s.ytimg.com
 50      content-delivery(65 ) 451 /0   C      3      s.ytimg.com
 50      content-delivery(65 ) 451 /0   C      3      s.ytimg.com

```

The following example displays the datapath IPv6 session statistics for WebCC counters:

```

(host) [mynode] (config) #show datapath session ipv6 web-cc counters

G - Global Counters
Datapath Session ipv6 WebCC counters
-----
Cpu  CategoryID  Category Name                Current Active Sessions  Total
Sessions
---  -
-----
G    0           Not Classified                0                          30812
G    2           computer/internet-security    0                          6
G    4           business-economy              0                          2050
G    5           computer/internet-info        0                          1032
G    7           shopping                      0                          2
G    9           travel                        0                          34
G   14           social-networking             0                          6
G   50           search-engines                0                          60
G   63           news/media                    0                          2

```

The following example displays the trusted and untrusted VLAN information:

```

(host) [mynode] #show datapath tunnel tunnel-id 17 trusted-vlan
Trusted Vlan(s):1-8,90-99,4093-4094

(host) [mynode] #show datapath tunnel tunnel-id 17 untrusted-vlan
Untrusted Vlan(s):9-89,100-4092

```

The following example displays the remote-user table entries,

```

(host) [mynode] #show datapath remote-user table ipv4
Remote User Entries
-----
Remote IP      ACL    Ver
-----

```

The following example displays information about next-hop devices for IPv6 address:

```
(host) [mynode] #show datapath nexthop-list ipv6
Datapath Nexthop List Table Entries
-----
Dest   Version  Nexthop                               Nexthop Dest  Nexthop Index  Nexthop
Version Nexthop  VLAN  Nexthop Priority                       -----
-----
0x4402 0x7      2620:11d:6038:102::2005 0x4422        0x002          0x6
          2011          128
```

The following example displays the datapath IPsec map details:

```
(host) [mynode] #show datapath ipsec-map
Datapath Nexthop List Table Entries
-----
Map Id  Map Dest  Tunnel Id  VLAN  Version  Updates  IP ver
-----
3       0x4622   0x10009   0     0x1     1        v6
4       0x4623   0x1000d   0     0x3     1        v6
5       0x4624   0x10011   193   0x5     1        v4
-----
Total Datapath Ipsec Map Table Entries: 3
```

The following output displays the next-hop list index for IPv6 policy-based routing:

```
(host) [mynode]#show datapath session ipv6 verbose

Datapath Session Table Entries
-----

Flags: F - fast age, S - src NAT, N - dest NAT
       D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS
       C - client, M - mirror, V - VOIP
       Q - Real-Time Quality analysis
       u - Upstream Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       r - Route Nexthop, h - High Value
       A - Application Firewall Inspect
       J - SDWAN Default Probe stats used as fallback
       B - Permanent, O - Openflow
       L - Log, o - Openflow config revision mismatched

Session Index, Route/Cache Index, Agg. Version Number[SIDX SRTI SRCI SRTRCV]

Source IP                               Destination IP
Prot SPort DPort Cntr      Prio ToS Age Destination TAge Packets  Bytes
SIDX  SRTI SRCI  SRTRCV  UsrIdx UsrVer  AclVer  NhlIdx
NhIdx  NhlNhVer  Flags                                CPU ID
-----
```

```

-----
-----
-----
2001:1:1:67:a9e9:41fc:92a0:2216          2001:1:1:568::251
 58  46218 32768 0/0      0  0  1  nh 0x4424  7  1  40
 53e   0   0      0      17  1127  dd3  2  4
 cdd   FCIr          6
2001:1:1:568::251          2001:1:1:67:a9e9:41fc:92a0:2216
 58  46211 33024 0/0      0  0  1  nh 0x4420  10 1  40
 91f   13  15      5f6b  0  0  0  0  0  0
 0     FI          6
-----
-----

```

The following output displays the next-hop lists for IPv6 policy-based routing:

```

(host) [mynode] #show datapath next-hop list ipv6
Datapath Nexthop List Table Entries
-----
Dest Version Nexthop Nexthop Dest Nexthop Index Nexthop Version Nexthop VLAN
Nexthop Priority
-----
-----
0x4401 0x3 2620::05 0x4421      0x001      0x2      4022
 *128

```

Related Commands

Command	Description
datapath	This command configures datapath options.

Command History

Release	Modification
ArubaOS 8.8.0.0	A new parameter, <code>allowed-address-list</code> was added.
ArubaOS 8.7.0.0	The command outputs are modified to include the following: <ul style="list-style-type: none"> A new flag, X is introduced for <code>show datapath tunnel</code> command. The <code>show datapath session dpi</code> command displays the AirSlice ID.
ArubaOS 8.6.0.0	The following changes were introduced:

Release	Modification
	<ul style="list-style-type: none"> ▪ The <code>remote-user table</code> parameter was added. ▪ The ipv6 option was added to the <code>nexthop-list</code> sub-parameter. ▪ The output of the <code>show datapath session ipv6</code> command was modified to display the next-hop list details, and includes the NhIIdx, NhIdx, and NhINhVer columns. ▪ The output of the <code>show datapath ipsec-map</code> command was modified to display v6 value under IP ver column.
ArubaOS 8.4.0.0	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ▪ The output of the <code>#show datapath tunnel ipv6</code> command was modified to include B, G, and Y flags. ▪ The output of the <code>show datapath route ap-name <ap-name> ipv6</code> and <code>show datapath route-cache ap-name <ap-name> ipv6</code> commands was modified to display IPv6 route entries. ▪ The <code>web-cc</code> and <code>counters</code> sub-parameters were added to <code>ipv6</code> parameter. ▪ The output of the <code>show datapath session ipv6 web-cc</code> command was modified to display WebCC related entries for IPv6 sessions. ▪ The <code>trusted-vlan</code> and <code>untrusted-vlan</code> sub-parameters were introduced in the <code>show datapath tunnel tunnel-id <id></code> command.
ArubaOS 8.2.0.0	The <code>netdest-id</code> , and <code>remote-device-table</code> parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show datapath cluster details

show datapath cluster details
peer <peer ip>

Description

Displays the following information:

- Global data - Heartbeat threshold values, databath assignments, and number of peers.
- Peer data - Peer statistics for cluster heartbeat requests sent, responses received, and heartbeats missed, and so on.

Parameter	Description
peer <peer ip>	Displays peer data statistics

Example

An example output of the show datapath cluster details command.

```
#show datapath cluster details

Datapath Cluster Heartbeat Data
=====
Datapath Bootup Time           = Mon May 11 22:17:00 2020
Current Timestamp              = Wed May 20 03:00:18 2020
Threshold                      = 1000 ms
Total Threshold Updates       = 1
Add Peer Requests to Datapath = 2
Del Peer Requests to Datapath = 0
HBT Request dropped as cluster disabled = 0
HBT Request dropped for non existent peers = 0
HBT Response dropped for non existent peers = 0
FP CPU                         = 10
Valid Peer count              = 2
Peer 00: (10.16.147.131)
=====
Did it ever connect           = yes
Is peer heartbeating         = yes
Current Uptime                = 7 days 1 hours 24 minutes 35
seconds
Last connect time            = Wed May 13 01:35:43 2020
Current Downtime             = N.A.
Last Disconnect Time         = Wed May 13 01:34:29 2020
Last disconnect sequence number = 1044965
Connect req to cp            = 3
Connect ack from cp          = 3
Disconnect req to cp         = 2
```

```

Disconnect ack from cp = 2
HBT Requests Sent (Curr,Total) = 6505338, 7550322
HBT Responses Rcvd (Curr,Total) = 6505321, 7550264
HBT Inflight or Drops (Curr,Total) = 17, 58
HBT Requests Rcvd (Curr,Total) = 6505201, 7550124
HBT Responses Sent (Curr,Total) = 6505201, 7550124
HBT Drops 'ReqRcvd-RespSent'(Curr,Total) = 0, 0
HBT Request Sent Sequence Number = 7550324
HBT Request Sent Timestamp = Wed May 20 03:00:18 2020
HBT Response Rcvd Sequence Number = 7550324
HBT Response Rcvd timestamp = Wed May 20 03:00:18 2020
Peer last HBT request rcvd sequence number = 7550164
Peer last HBT request rcvd timestamp = Wed May 20 03:00:18 2020
Peer HBT request missed count = 41
Delayed Response Rcvd Packets = 0
Last Delayed Response Sequence Number = 0
Last Delayed Response Timestamp = N.A.
Missed HBT response rcvd packets = 58
Missed HBT response rcvd Last sequence number = 0
Missed HBT response rcvd Last timestamp = N.A.
Peer disabled HBT Request Not Sent = 2215
Peer disabled HBT Request rcvd dropped = 0
Peer disabled HBT response rcvd dropped = 0

```

Missed Sequence Numbers:

=====

```

seq_no[995588] tx=Wed May 13 00:15:04 2020
seq_no[995589] tx=Wed May 13 00:15:04 2020
seq_no[995590] tx=Wed May 13 00:15:04 2020
seq_no[995591] tx=Wed May 13 00:15:04 2020
seq_no[995592] tx=Wed May 13 00:15:04 2020
seq_no[995593] tx=Wed May 13 00:15:04 2020
seq_no[995594] tx=Wed May 13 00:15:04 2020
seq_no[995595] tx=Wed May 13 00:15:05 2020
seq_no[1044966] tx=Wed May 13 01:34:27 2020
seq_no[1044967] tx=Wed May 13 01:34:27 2020
seq_no[1044968] tx=Wed May 13 01:34:27 2020
seq_no[1044969] tx=Wed May 13 01:34:27 2020
seq_no[1044970] tx=Wed May 13 01:34:27 2020
seq_no[1044971] tx=Wed May 13 01:34:28 2020
seq_no[1044972] tx=Wed May 13 01:34:28 2020
seq_no[1044973] tx=Wed May 13 01:34:28 2020
seq_no[1044974] tx=Wed May 13 01:34:28 2020
seq_no[1044975] tx=Wed May 13 01:34:28 2020
seq_no[1044976] tx=Wed May 13 01:34:28 2020
seq_no[1044977] tx=Wed May 13 01:34:28 2020
seq_no[1044978] tx=Wed May 13 01:34:28 2020
seq_no[1044979] tx=Wed May 13 01:34:28 2020
seq_no[1044980] tx=Wed May 13 01:34:28 2020
seq_no[1044981] tx=Wed May 13 01:34:28 2020
seq_no[1044982] tx=Wed May 13 01:34:29 2020
seq_no[1044983] tx=Wed May 13 01:34:29 2020
seq_no[1044984] tx=Wed May 13 01:34:29 2020
seq_no[1044985] tx=Wed May 13 01:34:29 2020
seq_no[1107017] tx=Wed May 13 03:12:38 2020
seq_no[1107018] tx=Wed May 13 03:12:38 2020
seq_no[1107019] tx=Wed May 13 03:12:38 2020

```

```
seq_no[1107020] tx=Wed May 13 03:12:39 2020
seq_no[1107021] tx=Wed May 13 03:12:39 2020
seq_no[1107022] tx=Wed May 13 03:12:39 2020
seq_no[1107023] tx=Wed May 13 03:12:39 2020
seq_no[1107024] tx=Wed May 13 03:12:39 2020
seq_no[1107025] tx=Wed May 13 03:12:39 2020
seq_no[1107026] tx=Wed May 13 03:12:39 2020
seq_no[1107027] tx=Wed May 13 03:12:39 2020
seq_no[1107028] tx=Wed May 13 03:12:39 2020
seq_no[1107029] tx=Wed May 13 03:12:39 2020
seq_no[1107030] tx=Wed May 13 03:12:39 2020
seq_no[1107031] tx=Wed May 13 03:12:40 2020
seq_no[1107032] tx=Wed May 13 03:12:40 2020
seq_no[1156039] tx=Wed May 13 04:29:14 2020
```

Delayed Sequence Numbers:

=====

RTD for Cluster heartbeat:

=====

seq_no = 7550324 min_rtd = 2 ms

seq_no = 7550324 max_rtd = 2 ms

avg_rtd = 2 ms

Missed Heartbeat request for Cluster heartbeat:

=====

Time: Mon May 11 22:17:00 2020 Missed_req_range: 995554 - 995573

Time: Mon May 11 22:17:00 2020 Missed_req_range: 1044943 - 1044963

Peer 01: (10.16.147.132)

=====

```
Did it ever connect           = yes
Is peer heartbeating         = yes
Current Uptime                = 1 hours 47 minutes 30
seconds
Last connect time            = Wed May 20 01:12:48 2020
Current Downtime             = N.A.
Last Disconnect Time         = Fri May 15 00:28:22 2020
Last disconnect sequence number = 1647427
Connect req to cp            = 2
Connect ack from cp          = 2
Disconnect req to cp         = 0
Disconnect ack from cp       = 0
HBT Requests Sent (Curr,Total) = 68806, 1716254
HBT Responses Rcvd (Curr,Total) = 68806, 1716233
HBT Inflight or Drops (Curr,Total) = 0, 21
HBT Requests Rcvd (Curr,Total) = 68806, 1716203
HBT Responses Sent (Curr,Total) = 68806, 1716203
HBT Drops 'ReqRcvd-RespSent'(Curr,Total) = 0, 0
HBT Request Sent Sequence Number = 1716254
HBT Request Sent Timestamp    = Wed May 20 03:00:18 2020
HBT Response Rcvd Sequence Number = 1716254
HBT Response Rcvd timestamp   = Wed May 20 03:00:18 2020
Peer last HBT request rcvd sequence number = 1716212
Peer last HBT request rcvd timestamp = Wed May 20 03:00:18 2020
Peer HBT request missed count = 10
Delayed Response Rcvd Packets = 0
Last Delayed Response Sequence Number = 0
Last Delayed Response Timestamp = N.A.
Missed HBT response rcvd packets = 20
```

```

Missed HBT response rcvd Last sequence number = 0
Missed HBT response rcvd Last timestamp      = N.A.
Peer disabled HBT Request Not Sent           = 4636439
Peer disabled HBT response rcvd dropped      = 19
Peer disabled HBT response rcvd dropped      = 0
Missed Sequence Numbers:
=====
seq_no[1647428] tx=Fri May 15 00:28:20 2020
seq_no[1647429] tx=Fri May 15 00:28:20 2020
seq_no[1647430] tx=Fri May 15 00:28:20 2020
seq_no[1647431] tx=Fri May 15 00:28:20 2020
seq_no[1647432] tx=Fri May 15 00:28:20 2020
seq_no[1647433] tx=Fri May 15 00:28:20 2020
seq_no[1647434] tx=Fri May 15 00:28:20 2020
seq_no[1647435] tx=Fri May 15 00:28:20 2020
seq_no[1647436] tx=Fri May 15 00:28:20 2020
seq_no[1647437] tx=Fri May 15 00:28:20 2020
seq_no[1647438] tx=Fri May 15 00:28:21 2020
seq_no[1647439] tx=Fri May 15 00:28:21 2020
seq_no[1647440] tx=Fri May 15 00:28:21 2020
seq_no[1647441] tx=Fri May 15 00:28:21 2020
seq_no[1647442] tx=Fri May 15 00:28:21 2020
seq_no[1647443] tx=Fri May 15 00:28:21 2020
seq_no[1647444] tx=Fri May 15 00:28:21 2020
seq_no[1647445] tx=Fri May 15 00:28:21 2020
seq_no[1647446] tx=Fri May 15 00:28:21 2020
seq_no[1647447] tx=Fri May 15 00:28:21 2020
Delayed Sequence Numbers:
=====
RTD for Cluster heartbeat:
=====
seq_no = 1716254 min_rtd = 2 ms
seq_no = 1716254 max_rtd = 2 ms
avg_rtd = 2 ms
Missed Heartbeat request for Cluster heartbeat:
=====
Time: Mon May 11 22:17:00 2020 Missed_req_range: 1647397 - 1647406

```

An example output of the show datapath cluster details peer command.

```

#show datapath cluster details peer 10.16.147.131
Peer 00: (10.16.147.131)
=====
Did it ever connect                = yes
Is peer heartbeating               = yes
Current Uptime                      = 7 days 1 hours 25 minutes 46
seconds
Last connect time                  = Wed May 13 01:35:42 2020
Current Downtime                   = N.A.
Last Disconnect Time               = Wed May 13 01:34:28 2020
Last disconnect sequence number    = 1044965
Connect req to cp                  = 3
Connect ack from cp                = 3

```



```

Disconnect req to cp = 2
Disconnect ack from cp = 2
HBT Requests Sent (Curr,Total) = 6506090, 7551074
HBT Responses Rcvd (Curr,Total) = 6506073, 7551016
HBT Inflight or Drops (Curr,Total) = 17, 58
HBT Requests Rcvd (Curr,Total) = 6505952, 7550875
HBT Responses Sent (Curr,Total) = 6505952, 7550875
HBT Drops 'ReqRcvd-RespSent'(Curr,Total) = 0, 0
HBT Request Sent Sequence Number = 7551076
HBT Request Sent Timestamp = Wed May 20 03:01:28 2020
HBT Response Rcvd Sequence Number = 7551076
HBT Response Rcvd timestamp = Wed May 20 03:01:28 2020
Peer last HBT request rcvd sequence number = 7550915
Peer last HBT request rcvd timestamp = Wed May 20 03:01:28 2020
Peer HBT request missed count = 41
Delayed Response Rcvd Packets = 0
Last Delayed Response Sequence Number = 0
Last Delayed Response Timestamp = N.A.
Missed HBT response rcvd packets = 58
Missed HBT response rcvd Last sequence number = 0
Missed HBT response rcvd Last timestamp = N.A.
Peer disabled HBT Request Not Sent = 2215
Peer disabled HBT Request rcvd dropped = 0
Peer disabled HBT response rcvd dropped = 0
Missed Sequence Numbers:

```

```

=====
seq_no[995588] tx=Wed May 13 00:15:03 2020
seq_no[995589] tx=Wed May 13 00:15:03 2020
seq_no[995590] tx=Wed May 13 00:15:03 2020
seq_no[995591] tx=Wed May 13 00:15:03 2020
seq_no[995592] tx=Wed May 13 00:15:03 2020
seq_no[995593] tx=Wed May 13 00:15:03 2020
seq_no[995594] tx=Wed May 13 00:15:03 2020
seq_no[995595] tx=Wed May 13 00:15:04 2020
seq_no[1044966] tx=Wed May 13 01:34:26 2020
seq_no[1044967] tx=Wed May 13 01:34:26 2020
seq_no[1044968] tx=Wed May 13 01:34:26 2020
seq_no[1044969] tx=Wed May 13 01:34:26 2020
seq_no[1044970] tx=Wed May 13 01:34:26 2020
seq_no[1044971] tx=Wed May 13 01:34:27 2020
seq_no[1044972] tx=Wed May 13 01:34:27 2020
seq_no[1044973] tx=Wed May 13 01:34:27 2020
seq_no[1044974] tx=Wed May 13 01:34:27 2020
seq_no[1044975] tx=Wed May 13 01:34:27 2020
seq_no[1044976] tx=Wed May 13 01:34:27 2020
seq_no[1044977] tx=Wed May 13 01:34:27 2020
seq_no[1044978] tx=Wed May 13 01:34:27 2020
seq_no[1044979] tx=Wed May 13 01:34:27 2020
seq_no[1044980] tx=Wed May 13 01:34:27 2020
seq_no[1044981] tx=Wed May 13 01:34:27 2020
seq_no[1044982] tx=Wed May 13 01:34:28 2020
seq_no[1044983] tx=Wed May 13 01:34:28 2020
seq_no[1044984] tx=Wed May 13 01:34:28 2020
seq_no[1044985] tx=Wed May 13 01:34:28 2020
seq_no[1107017] tx=Wed May 13 03:12:37 2020
seq_no[1107018] tx=Wed May 13 03:12:37 2020

```

```

seq_no[1107019] tx=Wed May 13 03:12:37 2020
seq_no[1107020] tx=Wed May 13 03:12:38 2020
seq_no[1107021] tx=Wed May 13 03:12:38 2020
seq_no[1107022] tx=Wed May 13 03:12:38 2020
seq_no[1107023] tx=Wed May 13 03:12:38 2020
seq_no[1107024] tx=Wed May 13 03:12:38 2020
seq_no[1107025] tx=Wed May 13 03:12:38 2020
seq_no[1107026] tx=Wed May 13 03:12:38 2020
seq_no[1107027] tx=Wed May 13 03:12:38 2020
seq_no[1107028] tx=Wed May 13 03:12:38 2020
seq_no[1107029] tx=Wed May 13 03:12:38 2020
seq_no[1107030] tx=Wed May 13 03:12:38 2020
seq_no[1107031] tx=Wed May 13 03:12:39 2020
seq_no[1107032] tx=Wed May 13 03:12:39 2020
seq_no[1156039] tx=Wed May 13 04:29:13 2020
Delayed Sequence Numbers:
=====
RTD for Cluster heartbeat:
=====
seq_no = 7551076 min_rtd = 2 ms
seq_no = 7551076 max_rtd = 2 ms
avg_rtd = 2 ms
Missed Heartbeat request for Cluster heartbeat:
=====
Time: Mon May 11 22:16:59 2020 Missed_req_range: 995554 - 995573
Time: Mon May 11 22:16:59 2020 Missed_req_range: 1044943 - 1044963

```

Related Commands

Command	Description
show lc-cluster	This command displays information related to vlan, membership, profile, heartbeat, and so on for a cluster.
show datapath cluster heartbeat counters	This command displays information related to cluster heartbeat counters.
show lc-cluster history	This command displays the history of the connection and disconnection events with a reason and the time stamp.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode or enable mode in the managed device.

show datapath cluster heartbeat counters

show datapath cluster heartbeat counters

Description

Displays information related to cluster heartbeat counters.

Example

An example output of the `show datapath cluster heartbeat counters` command.

```
#show datapath cluster heartbeat counters
Cluster Heartbeat Counters
-----
IPv6 Address                               RES      RSR      MIS      TOTRES
TOTRSR   TOTMIS   HMPD                               LTOD
-----
2000:10:17:65::55      1798     1798     0         1798     1798         0         0
Tue Feb 25 05:41:15 2020
2000:10:17:65::56         0         0         0         0         0         0         0
2000:10:17:65::57         0         0         0         0         0         0         0
-----
-----PREAMBLE-----
RES      - REQ SENT
RSR      - RSP RCVD
MIS      - MISSES
TOTRES   - TOTAL REQ SENT
TOTRSR   - TOTAL RSP RCVD
TOTMIS   - TOTAL MISSES
HMPD     - HBT MISS PEER DEAD
LTOD     - LAST TIME OF DISCONNECT
-----
```

Related Commands

Command	Description
show datapath cluster details	This command displays heartbeat threshold values, datapath assignments, number of peers and peer data statistics.
show lc-cluster	This command displays information related to vlan, membership, profile, heartbeat, and so on for a cluster.
show lc-cluster history	This command displays the history of the connection and disconnection events with a reason and the time stamp.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode or enable mode in the managed device.

show dds debug

```
global_object_db [peer <A.B.C.D> [rkey <rkey-id>] |peerv6 <X:X:X:X::X>]
message-stats
peers
rkey
replicaton <sources>
stats
```

Description

This command shows the dds debug information.

Parameter	Description
global_object_db	DDS global object database.
peer <A.B.C.D>	Peer for the global object database.
rkey <rkey-id>	Replication key for the global object database.
peerv6 <X:X:X:X::X>	Set peer ipv6 address.
message-stats	Message statistics.
peers	Remote peers.
replication	Object replication.
rkey <rkey-id>	Replication keys
stats	Statistics of the DDS log

Related Commands

Command	Description
dds trace	This command configures trace events.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>peerv6</code> parameter was added.

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show debug

show debug

Description

This command shows the debug information for debug logging levels.

Example

```
(host) [mynode] (config) #show debug
DEBUG LEVELS
-----
Facility      Level      Debug Value      Sub Category      Process
-----
user-debug    debugging  12:12:12:12:12   N/A                N/A
```

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show dot1x

```
show dot1x
  ap-hash-table
  ap-table
  certificates
  counters
  dot1x-counters
  eap-frag-mtu
  machine-auth-cache
  supplicant-info
  watermark
  wired-ap-table
```

Description

Shows the 802.1X related configurations.

Parameter	Description
ap-hash-table	Shows dot1x ap hash table.
ap-table	Shows 802.1X AP table.
certificates	Shows 802.1x certificate usage.
counters	Shows 802.1X counters.
dot1x-counters	Shows 802.1X counters.
eap-frag-mtu	Shows IP MTU for EAP fragmentation.
machine-auth-cache	Shows machine authentication cache.
supplicant-info	Shows details about supplicant(s).
watermark	Shows active and pending queue.
wired-ap-table	Shows 802.1X wired AP table.

Related Commands

Command	Description
dot1x	Use this command under the guidance of Aruba

Command	Description
	support to configure the maximum and minimum thresholds for the table that contains 802.1X sessions.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x ap-table

show dot1x ap-table

Description

Shows the 802.1X AP table.

Example

Issue this command to display details from the AP table.

```
AP Table
-----
MAC          IP          Essid          Type AP name          Vlan Enc
  Stations Forwarding-Mode  Profile          Acl
-----
00:1a:1e:87:ff:c0 10.3.9.242          AP 00:1a:1e:c0:7f:fc 0 -
0          FORWARD_TUNNEL_80211 default/          1
00:1a:1e:87:ff:d0 10.3.9.242 sw-pn-nokia AP 00:1a:1e:c0:7f:fc 0 WPA2-
AES 0          FORWARD_TUNNEL_80211 default/default 1
00:1a:1e:82:ab:a0 10.3.9.220          AP monitor-124          0 -
0          FORWARD_TUNNEL_80211 default/          1
00:1a:1e:82:ab:b0 10.3.9.220          AP monitor-124          0 -
0          FORWARD_TUNNEL_80211 default/          1
00:1a:1e:87:ff:d1 10.3.9.242 sw-pn-t2 AP 00:1a:1e:c0:7f:fc 0 WPA2-
PSK-AES 0          FORWARD_TUNNEL_80211 default/default 1
Num APs: 5
```

The output of this command includes the following parameters:

Parameter	Description
MAC	The MAC address of the AP
IP	The IP address of the AP
Essid	The AP's ESSID
Type	Device type
AP name	Name of the AP
Vlan	Number of VLANs associated with the specified AP
Enc	AP's encryption method

Parameter	Description
Stations	Number of stations associated with the specified AP
Forwarding Mode	Forwarding mode used by the specified AP
Profile	AP profile
Acl	Number of ACLs this AP belongs to

Related Commands

Command	Description
dot1x	Use this command under the guidance of Aruba support to configure the maximum and minimum thresholds for the table that contains 802.1X sessions.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x ap-table aes

```
show dot1x ap-table aes
```

Description

Shows the AES keys of all APs.

Example

Issue this command to display AES keys of all APs.

```
AP Table Showing AES Keys
-----
AP-MAC          GTK/Size/Slot
-----
00:1a:1e:87:ff:d0 * * * * * */128-Bit/1
00:1a:1e:87:ff:d1 * * * * * */128-Bit/1
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP MAC address
GTK/Size/Slot	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Related Commands

Command	Description
wlan ssid-profile	This command configures an SSID profile.
show wlan ssid-profile	This command displays the list of all SSID profiles, or detailed configuration information for a specific SSID profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x ap-table dynamic-wep

```
show dot1x ap-table dynamic-wep
```

Description

Shows the dynamic WEP keys of all APs.

Example

Issue this command to display dynamic keys of all APs.

```
Dynamic-WEP Key Information
-----
AP-MAC  Key1/Size/Slot  Key2/Size/Slot
-----  -----
Num APs: 0
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP MAC address
Key1/Size/Slot	Key1: The WEP key Size: Size of the WEP key Slot: Slot number
Key12/Size/Slot	Key2: The WEP key Size: Size of the WEP key Slot: Slot number

Related Commands

Command	Description
aaa authentication dot1x	This command configures the 802.1X authentication profile.
show dot1x certificate details	Displays a detailed 802.1X certificate usage.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x ap-table static-wep

show dot1x ap-table static-wep

Description

Shows the static WEP keys of all APs.

Example

Issue this command to display the static WEP keys of all APs.

```
Static-WEP Key Information
-----
AP-MAC  Key1/Size  Key2/Size  Key3/Size  Key3/Size
-----  -
Num APs: 0
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP's MAC address
Key1/Size	WEP key 1 and its size
Key2/Size	WEP key 2 and its size
Key3/Size	WEP key 3 and its size
Key3/Size	WEP key 3 and its size

Related Commands

Command	Description
ap wifi-uplink-profile	This command configures a Wi-Fi uplink profile.
show ap config	Shows a large list of configuration settings for an ap-group or an individual AP.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x ap-table tkip

```
show dot1x ap-table tkip
```

Description

Displays a table of TKIP keys on the managed devices.

Example

Issue this command to display all TKIP keys.

```
AP Table Showing TKIP Keys
-----
AP-MAC                GTK/Size/Slot
-----
00:1a:1e:6f:e5:10    * * * * * */256-Bit/1
Num APs: 1
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP MAC Address
GTK/Size/Slot	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Related Commands

Command	Description
wlan ssid-profile	This command configures an SSID profile.
wlan ht-ssid-profile	This command configures a high-throughput SSID profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x dot1x-counters

show dot1x dot1x-counters

Description

Displays a table of dot1x counters.

Example

Issue this command to display all 802.1X counter information.

```

802.1x Counters
Dot1x auth pass count.....0
Dot1x auth fail count.....0
Double dot1x context init counts.....0/0
Current Time : Mar  9 00:53:04 Blocking measured for 3467857 sec & 321635
usec, total ticks = 3467857321
Error (diff < 0) counter = 0, gsm_tick_resolution_in_microseconds = 1000
Blocking Call times
-----
function-name          #calls Total #ticks max #ticks <1ms ~2ms ~4ms
~8ms ~16ms ~32ms ~64ms ~128ms ~256s >256ms  ----  ----  ----
-----
station_delete_sibyte  0      0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
user_download          0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
l3user_download       0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
user_delete_sessions   0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
user_delete_sibyte     0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
send_dp_aes_key        0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
send_dp_key            0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0
send_station_dataready 0      0      0      0      0      0      0      0
0      0      0      0      0      0      0      0      0

```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x ap-hash-table

show dot1x ap-hash-table

Description

Shows the 802.1X ap hash table.

Related Commands

Command	Description
aaa authentication dot1x	This command configures the 802.1X authentication profile.
show dot1x certificate details	Displays a detailed 802.1X certificate usage.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x certificate details

show dot1x certificates details

Description

Displays a detailed 802.1X certificate usage.

Example

```
(host) [mynode] (config) #show dot1x certificates details

Certificate Hash table entries
-----
Certificate Name: default-self-signed
Usage Count: 3, Dot1x:Yes, Captive portal:No, Ldap:No
Dot1x certificate table entries
-----
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x counters

show dot1x counters

Description

Displays a table of dot1x counters.

Example

Issue this command to display all 802.1X counter information.

```
802.1X Counters

AP
  Sync Request.....4
  Sync Response.....3
  Up.....4
  Down.....1
  Resps.....4
  Acl.....53
Station
  Sync Request.....9
  Sync Response.....9
  Up.....2321
  Down.....2272
  Unknown.....72
EAP
  RX Pkts.....4811
  Dropped Pkts.....4497
  TX Pkts.....5253
WPA
  Message-1.....2484
  Message-2.....63
  Message-3.....63
  Message-4.....63
  Group Message-1.....63
  Group Message-2.....63
  Rx Failed.....2418
  IE Mismatches.....4836
  Key Exchange Failures.....602
WPA2
  Message-1.....2630
  Message-2.....13
  Message-3.....13
  Message-4.....13
  Rx Failed.....2079
  IE Mismatches.....4158
  Key Exchange Failures.....549
Radius
  Accept.....1217
  Station Deaths.....1151
```


The output of this command includes the following parameters:

Parameter	Description
AP <ul style="list-style-type: none"> ■ Sync Request ■ Sync Response ■ Up ■ Down ■ Resps ■ Acl 	<ul style="list-style-type: none"> ■ Number of sync requests sent ■ Number of sync responses sent ■ Number of times an AP has come up ■ Number of times an has gone down ■ Number of response messages sent to the AP due to an AP up message ■ Number of ACLs
Station <ul style="list-style-type: none"> ■ Sync Request ■ Sync Response ■ Up ■ Down ■ Unknown 	<ul style="list-style-type: none"> ■ Number of sync requests sent to find all APs and stations that are connected ■ Number of sync responses received ■ Number of times a station (any station) connected to the AP ■ Number of times a station (any station) disconnected from the AP ■ Number of times a station attempted to start an EAP exchange before associating to an AP. In other words, the number of times the auth module saw the start of an EAP exchange before auth was notified that a station has associated an AP
EAP <ul style="list-style-type: none"> ■ RX Pkts ■ Dropped Pkts ■ TX Pkts 	<ul style="list-style-type: none"> ■ Number of EAP packets received ■ Number of EAP packets dropped (ignored) for any reason, such as bad packet, length, EAP ID mismatch, etc. ■ Number of EAP packets sent
WPA <ul style="list-style-type: none"> ■ Message-1 ■ Message-2 ■ Message-3 ■ Message-4 ■ Group Message-1 ■ Group Message-2 ■ Rx Failed ■ IE Mismatches ■ Key Exchange Failures 	<ul style="list-style-type: none"> ■ Number of WPA message-1s sent ■ Number of WPA message-2s sent ■ Number of WPA message-3s sent ■ Number of WPA message-4s sent ■ Number of WPA group message-1s sent ■ Number of WPA group message-2s sent ■ Number of WPA related EAP packets dropped for any reason ■ Number of WPA related EAP packets dropped because the station and controller have a different perception of what

Parameter	Description
	<p>the connection details are</p> <ul style="list-style-type: none"> Number of key exchange failures
WPA2 <ul style="list-style-type: none"> Message-1 Message-2 Message-3 Message-4 Rx Failed IE Mismatches Key Exchange Failures 	<ul style="list-style-type: none"> Number of WPA2 message-1s sent Number of WPA2 message-2s sent Number of WPA2 message-3s sent Number of WPA2 message-4s sent Number of WPA2 related EAP packets dropped for any reason Number of WPA2 related EAP packets dropped because the station and controller have a different perception of what the connection details are Number of key exchange failures
Radius Accept	Number of RADIUS accepts
Station Deaths	Number of stations deaths

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x eap-frag-mtu

show dot1x eap-frag-mtu

Description

Displays the IP MTU to be considered for EAP fragmentation.

Example

```
(host) [mynode] (config) #show dot1x eap-frag-mtu
DOT1x EAP Fragmentation MTU.....1000
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show dot1x machine-auth-cache

```
show dot1x machine-auth-cache <supplicant-mac>
```

Description

Shows the machine authentication cache.

Related Commands

Command	Description
show aaa authentication dot1x	This command shows information for 802.1X authentication profiles.
show aaa authentication mac	This command shows information for MAC authentication profiles.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x supplicant-info

```
list-all
pmkid
reauth-table
statistics
<supplicant-mac>
```

Description

Shows the details about a supplicant.

Parameter	Description
list-all	Show all 802.1X supplicants.
pmkid	Show pmkids of the stations.
reauth-table	Shows the reauthentication related information.
statistics	Show 802.1X statistics of the users.

Example

Issue this command to display the details about a supplicant.

Name	MYCORPNETWORKS\ccutler
MAC Address	00:19:7e:a9:8e:b0
AP MAC Address	00:1a:1e:11:5f:11
Status	Authentication Success
Unicast Cipher	WPA2-AES
Multicast Cipher	WPA2-AES
EAP-Type	EAP-PEAP
Packet Statistics:	
EAPOL Starts	0
EAP ID Requests	0
EAP ID Responses	0
EAPOL Logoffs from station	0
EAP pkts to the station	2
EAP pkts from station	2
Unknown EAP pkts from station	0
EAP Successes sent	0
EAP Failures sent	0
Station failed to respond	0
Station NAKs	0
Radius pkts to the server	0
Radius pkts from the server	0
Server failed to respond	0
Server rejects	0

```

WPA/WPA2-Key Message1      1
WPA/WPA2-Key Message2      1
WPA/WPA2-Key Message3      1
WPA/WPA2-Key Message4      1
WPA-GKey Message1          0
WPA-GKey Message2          0
ID of the last EAP request   0
Length of the last EAP request 151
ID of the last EAP response  0
Length of the last EAP response 0
ID of the last radius request 0
Length of the last radius request 0
ID of the last radius response 0

```

The output of this command includes the following parameters:

Parameter	Description
Name	Supplicant name.
MAC Address	Supplicant MAC address.
AP MAC Address	AP MAC address.
Status	Supplicant's status.
Unicast Cipher	Supplicant's unicast cipher.
Multicast Cipher	Supplicant's multicast cipher.
EAP-Type	Supplicant's EAP-Type.
EAPOL Starts	Number of EAPOL starts.
EAP ID Requests	Number of EAP ID requests.
EAP ID Responses	Number of EAP ID responses.
EAPOL Logoffs from station	Number of EAPOL logoffs from the station.
EAP pkts to the station	Number of EAP packets sent to the station.
EAP pkts from station	Number of EAP packets sent from the station.
Unknown EAP pkts from station	Number of unknown EAP packets sent from the station.
EAP Successes sent	Number of EAP successes sent.
EAP Failures sent	Number of EAP failures sent.

Parameter	Description
Station failed to respond	Number of times the station failed to respond.
Station NAKs	Number of station negative-acknowledgement characters.
Radius pkts to the server	Number of RADIUS packets set to the server.
Radius pkts from the server	Number of RADIUS packets sent from the server.
Server failed to respond	Number of times the server failed to respond.
Server rejects	Number of times a connection was rejected by the server.
WPA/WPA2-Key Message1	Number of WPA message-1s sent
WPA/WPA2-Key Message2	Number of WPA message-2s sent.
WPA/WPA2-Key Message3	Number of WPA message-3s sent.
WPA/WPA2-Key Message4	Number of WPA message-4s sent.
WPA-GKey Message1	Number of WPA group message-1s sent.
WPA-GKey Message2	Number of WPA group message-2s sent.
ID of the last EAP request	The ID of the last EAP request.
Length of the last EAP request	The length of the last EAP request.
ID of the last EAP response	The ID of the last EAP response.
Length of the last EAP response	The length of the last EAP response.
ID of the last radius request	The ID of the last RADIUS request.
Length of the last radius request	The length of the last RADIUS request.
ID of the last radius response	The ID of the last RADIUS response.
Length of the last radius response	The length of the last RADIUS response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x supplicant-info list-all

```
show dot1x supplicant-info list all
```

Description

Shows all 802.1X supplicants.

Syntax

No parameters.

Example

Issue this command to display all 802.1X supplicants as well as additional relevant information.

```
802.1X User Information
-----
      MAC           Name      Auth  AP-MAC           Enc-Key/Type
      Auth-Mode     EAP-Type Remote
-----
00:15:00:26:f8:f5  user1    Yes  00:0b:86:8b:68:68  * * * * * */WPA2-
AES Explicit Mode  EAP-PEAP  No
Station Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
Auth	Shows if the supplicant authenticated successfully
AP-MAC	AP MAC address
Enc-Key/Type	Enc-Key: Supplicant's encryption key Type: Encryption type used by the supplicant
Auth-Mode	Authentication mode
EAP-Type	EAP type
Remote	Is the supplicant remote

Related Commands

Command	Description
show dot1x supplicant-info	This command shows the details about a specific supplicant.
show dot1x supplicant-info pmkid	This command shows the PMKIDs of the various stations on the controller.
show dot1x supplicant-info statistics	This command shows the 802.1X statistics of the users.
show dot1x supplicant-info reauth-table	This command shows the reauthentication related information.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x supplicant-info pmkid

```
show dot1x supplicant-info pmkid <supplicant-mac>
```

Description

Shows the PMKIDs of the various stations on the controller.

Syntax

No parameters.

Example

Issue this command to display the PMKIDs of the various stations on the controller.

```
PMKID Table
-----
Mac                Name                AP                PMKID
---                -
00:03:7f:bf:12:ac  zoobar22            00:0b:86:a0:57:60
c2:7d:12:1a:1c:5b:40:f8:89:46:22:a5:ec:9b:fb:a6
00:03:7f:bf:12:ac  zoobar22            00:0b:86:c0:04:88
bb:2d:e1:57:e1:b8:9b:a2:71:f5:98:ad:61:db:47:e7
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
AP	AP MAC address
PMKID	Station PMKID

Related Commands

Command	Description
show dot1x supplicant-info	This command shows the details about a specific supplicant.

Command	Description
show dot1x supplicant-info list-all	This command shows all 802.1X supplicants.
show dot1x supplicant-info statistics	This command shows the 802.1X statistics of the users.
show dot1x supplicant-info reauth-table	This command shows the reauthentication related information.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x supplicant-info statistics

```
show dot1x supplicant-info statistics
```

Description

Shows the 802.1X statistics of the users.

Syntax

No parameters.

Example

Issue this command to display the 802.1X statistics of the users.

```
802.1X Statistics
-----
Mac          Name  AP          Auth-Succs  Auth-Fails  Auth-
Tmout  Re-Auths  Supp-Naks  UKeyRotations  MKeyRotations
---          -
00:15:00:26:f8:f5  user1  00:0b:86:8b:68:68  1          0          0
0          0          0          0          0
Total:
0          0          0          0          2          0          0

Station Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address.
Name	Supplicant name.
AP	AP MAC address.
Auth-Succs	Number of successful authentications.
Auth-Fails	Number of authentication failures.
Auth-Tmout	Number of authentication timeouts.
Re-Auths	Number of reauthentications.

Parameter	Description
Supp-Naks	Number of negative-acknowledgement characters sent by the supplicant.
UKeyRotations	Number of unicast key rotations.
MKeyRotations	Number of multicast key rotations.

Related Commands

Command	Description
show dot1x supplicant-info	This command shows the details about a specific supplicant.
show dot1x supplicant-info list-all	This command shows all 802.1X supplicants.
show dot1x supplicant-info pmkid	This command shows the PMKIDs of the various stations on the controller.
show dot1x supplicant-info reauth-table	This command shows the reauthentication related information.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x supplicant-info reauth-table

```
show dot1x supplicant-info reauth-table [all|history|mac]
```

Description

Shows the reauthentication related information.

Syntax

Parameter	Description
all	All entries in reauth-table.
history	Information about last few reauth sweeps.
mac	Supplicant MAC address.

Command History

Version	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x watermark

```
crypto-local
show dot1x watermark
  history
  table {active|pending}
```

Description

Use this command under the guidance of Aruba support to view information about the table that contains 802.1X sessions being processed.

Syntax

Parameter	Description
history	Displays all historical sessions in the 802.1X session queue.
table {active pending}	Table types: <ul style="list-style-type: none">■ active: Displays all current active sessions in the 802.1X queue and the corresponding user-age.■ pending: Displays all pending sessions in the 802.1X queue, the duration for which the user is pending in the queue, and the corresponding user-age.

Related Commands

Command	Description
dot1x	This command is used to configure the maximum and minimum thresholds for the table that contains 802.1X sessions.
show rf event-thresholds-profile	This command shows an event threshold profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show dot1x wired-ap-table

show dot1x wired-ap-table

Description

Shows the 802.1X Wired AP table.

Syntax

No parameters.

Command History

Version	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show dot1x-transactions-monitor

```
show dot1x-transactions-monitor stats
```

Description

This command displays the rate statistics, per second, for a 802.1X user. The command output is displayed only when the interval and duration is set in the `dot1x-transactions-monitor set` command, and the start action is executed in the `dot1x-transactions-monitor` command.

Parameter	Description
stats	<p>Displays the 802.1X rate statistics, per second. The output of the command displays Interval, Success, Failure, Dot1x-Station-Up, EAP-Request-Sent, EAP-Response-Received, Radius-Request-Sent, and Radius-Response-Received per second in each interval.</p> <p>NOTE: To stop the running statistics, execute the stop parameter under the <code>dot1x-transactions-monitor</code> command.</p>

Example

The output of the `show dot1x-transactions-monitor` command displays the rate statistics for the 802.1X users:

```
(host) [mynode] #show dot1x-transactions-monitor stats
802.1x Rate Statistics (All numbers are per second in each interval)
-----
Interval Success Failure Dot1x-Station-Up EAP-Request-Sent EAP-Response-
Received Radius-Request-Sent Radius-Response-Received
-----
1 0.0889 0.0000 0.0889 1.2444 1.1556 0.9778 0.9778
2 0.0444 0.0000 0.0444 0.6222 0.5778 0.4889 0.4889
3 0.0444 0.0000 0.0444 0.6222 0.5778 0.4889 0.4889
4 0.0444 0.0000 0.0444 0.6222 0.5778 0.4889 0.4889
5 0.2000 0.0000 0.2000 2.8000 2.6000 2.2000 2.2000
```

Related Commands

Command	Description
<u>dot1x-transactions-monitor</u>	Starts or stops the display of the rate statistics using the <code>show dot1x-transactions-monitor</code> command.
<u>dot1x-transactions-monitor set</u>	Sets the rate statistics interval duration and the total duration of a 802.1X transaction.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show dpi

```
show dpi
application
  name
  all
  category <name>
  custom-app <name>
global-bandwidth-contract
  all
  category <name>
  custom-app <name>
custom-app
  all
  string
```

Description

Shows applications and application categories that are configured for DPI. It also shows DPI global bandwidth contracts by application or application category.

Syntax

Parameter	Description
name	Name of the application.
all	Shows all applications.
category <name>	Shows all applications within a category.
custom-app <name>	Shows all custom applications.
global-bandwidth-contract	Shows the DPI global bandwidth contracts.
all	Shows all bandwidth contracts.
app <name>	Shows bandwidth contracts by application name.
appcategory <name>	Shows bandwidth contracts by application category name.
custom-app	Show custom applications.
all	Show all applications.
string	Name of the application to show.

Example

The output of the following command shows custom applications by name, ID, application category, and default ports that are configured for DPI.

```
(host) (config) #show dpi application all
Applications
-----
Name                               App ID  App Category      Default Ports
Applied
-----
-----
01net                               948     web                tcp 80
0
050plus                             1123    audio-video       tcp 80 443
0
0zz0                                584     web                tcp 80
0
10050net                            1339    web                tcp 80
0
10086cn                              949     web                tcp 80 443
0
104com                              1336    web                tcp 80
0
1111tw                              1338    web                tcp 80
0
1141a                               950     web                tcp 80
0
115com                              951     web                tcp 80 443
0
118114cn                           952     web                tcp 80
0
11st                                1191    web                tcp 80
0
```

Related Commands

Command	Description
dpi	Use this command to configure DPI and the global bandwidth contract for an application or application categories for the AppRF feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show esi

Syntax

```
groups [{group-name <groupname>|{ping-name <ping-name>}}]  
parser domains|rules|stats  
ping [ping-name <ping-name>]  
servers [{group-name <groupname>|{server-name <server-name>}}]
```

Description

Displays ESI group, parser, ping health check settings, and configuration information for ESI servers.

Parameter	Description
<u>groups</u> group-name ping-name	Shows ESI group information.
<u>parser</u> domains rules stats	Shows ESI parser information.
<u>ping</u> ping-name	Shows settings for ESI ping health check attributes.
<u>servers</u> server-name	Show configuration information for ESI servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show esi groups

```
show esi groups [{group-name <groupname>|{ping-name <ping-name>}]
```

Description

Show ESI group information. The ESI parser is a mechanism for interpreting syslog messages from third party appliances such as anti-virus gateways. Use this command to view configured ESI server groups.

Parameter	Description
group-name <groupname>	View the facility used when logging messages into the remote syslog server.
ping-name <ping-name>	Enter the name of a set of ping values to how the names of ESI groups using that set of ping attributes. Define a set of ESI ping values using the command esi ping .

Example

This example below displays the name of each configured ESI group, including its ping definitions and ESI server.

```
(host) #show esi groups

ESI Group Table
-----
Name          Tunnel ID  Ping      Flags  Servers
----          -
anything      0x1042    pingset_1 C       0
cupertino     0x1043    -         C       0
Flags:
  C:Datapath Download complete
```

Related Commands

Platforms	Licensing	Command Mode
esi parser domain	This command configures an ESI syslog parser domain.	Config mode on Mobility Conductor

Platforms	Licensing	Command Mode
esi parser rule	This command creates or changes an ESI syslog parser rule.	Config mode on Mobility Conductor

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show esi parser

```
show esi parser domains|rules|stats
```

Description

Shows ESI parser information. The ESI parser is a generic syslog parser on the controller that accepts syslog messages from external third-party appliances such as anti-virus gateways, content filters, and IDS. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users. ESI servers are configured into domains to which ESI syslog parser rules are applied.

Parameter	Description
domains	Show ESI parser domain information.
rules	Show ESI parser rule information.
stats	Show ESI parser rule stats.

Example

Use the `show esi parser domains` command to show ESI parser domain information.

The ESI Parser Domain table in the example below shows that the controller has two ESI domains and two ESI servers.

```
(host) [mynode] (config) #show esi parser domains

ESI Parser Domain Table
-----
Domain          ESI Servers   Peer controllers
-----
corp_domain     172.21.5.50   10.3.132.14
remote_domain   192.84.66.30

Total number of servers configured: 2
```

Related Commands

Platforms	Licensing
esi parser domain	This command configures an ESI syslog parser domain.
esi parser rule	This command creates or changes an ESI syslog parser rule.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show esi ping

```
show esi ping [ping-name <ping-name>]
```

Description

Show settings for ESI ping health check attributes.

Parameter	Description
ping-name <ping-name>	Include the optional ping-name <ping-name> parameters to display settings for one specified set of ping settings.

Example

This example below shows that the controller has three defined sets of ping attributes.

```
(host) #show esi groups

ESI Ping Table
-----
Name          Frequency (sec)  Timeout (sec)  Retry Count  ID  Num Groups
-----
ping_att1          5                5                2            2    2
ESIPing           50000            5                2            2    2
ESIPing2           50000            5                2            2    2
```

The output of this command includes the following information:

Column	Description
Name	Name of a group of ping settings.
frequency	Specifies the ping frequency in seconds.
timeout	Specifies the ping timeout in seconds.
retry-count	Specifies the ping retry count
ID	ID number assigned to the ping attributes when that set of attributes was defined.
Num Groups	Number of ESI groups to which this set of ping attributes is assigned.

Related Commands

Platforms	Licensing
esi ping	This command specifies the ESI ping health check configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show esi servers

```
show esi servers [{group-name <groupname>|{server-name <server-name>}]
```

Description

Show configuration information for ESI servers. By default, this command displays configuration settings for all ESI servers. You can include the name of an ESI group to view servers assigned to just that group, or specify a server name to view information for that server only.

Parameter	Description
server-name <server-name>	Specify an ESI server name to view configuration information for just that server.

Example

This example below displays configuration details for the ESI server name **forti_1**.

```
(host) #show esi servers server-name forti_1

ESI Server Table
-----
Name      Trusted IP      Untrusted IP    Trusted Port  Untrusted Port  Group  Mode
  NAT Port  ID
-----  -
-----  --
forti_1  10.168.173.2   10.168.171.3   -/-/-        -/-/-          default
route 0      4

Flags
-----
U

Flags:
C :Datapath Download complete
U :Server Up
D :Server Down
PT:Trusted Ping response outstanding
PU:Untrusted Ping response outstanding
HT:Health Check Trusted IP
HU:Health Check Untrusted IP
FT:Trusted Ping failed
FU:Untrusted Ping failed
```

The output of this command includes the following information:

Column	Description
Name	Name of the ESI server.
Trusted IP	Displays the server IP address on the trusted network. As an option, you can also enable a health check on the specified address
Untrusted IP	Displays the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address
Trusted Port	Shows the slot and port connected to the trusted side of the ESI server in the format <slot>/<module>/<port>.
Untrusted Port	Shows the slot and port connected to the untrusted side of the ESI server in the format <slot>/<module>/<port>.
Group	Name of the ESI group to which this server is assigned. If the server has not yet been assigned to a group, this column will be blank.
Mode	Specifies the ESI server mode of operation: bridge, nat, or route
Nat Port	Displays the NAT destination TCP or UDP port.
ID	ID number assigned to the server when it was first defined.
Flags	This data column displays any flags associated with this server. The flag key appears below the ESI Server Table.

Related Commands

Platforms	Licensing
esi server	This command configures an ESI server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show est

```
show est
  profile-name
  status [all]
```

Description

Displays information of the activated EST profiles. Click parameter links to view the corresponding show commands.

Parameter	Description
profile-name	Displays the information of the activated EST profiles on the device.
status	Displays the information of the activated EST profiles along with the current status of the EST information on the device.

Examples

The output of this command shows the current EST status of a single managed device:

```
(Host) [mynode] #show est profile test_profile
EST Profile "test_profile"
-----
Parameter                               Value
-----
Server Host                             10.15.100.142
Server Port                             443
Challenge password                       *****
Arbitrary label                          /ca:5
Server's CA Cert Name                    estcert
Organizational Unit Name                 N/A
Arbitrary enrollment label               N/A
Arbitrary reenrollment label             N/A
Username                                 N/A
Password                                 N/A
CSR attribute Config                     RSA_with_SHA256
```

The output of this command includes the following information:

Column	Description
Server Host	IP address of the managed device.
Server Port	Default port of the managed device or switch.

Column	Description
Challenge Password	Challenge password, if enabled.
Arbitrary label	
Server's CA Cert Name	Name of the server's CA certificate.
Organizational Unit Name	Name of the organization under which the server is hosted.
Arbitrary enrollment label	
Arbitrary reenrollment label	
Username	Username of the admin.
Password	Password of the admin.
CSR attribute Config	CSR attribute string (For example, RSA_with_SHA256)

The output of this command shows the current EST status of all the switches:

```
(host) [mynode] # show est status all
EST Status for All Switches
-----
IP Address      Name              Type      Version      Profile
Status          Expiry time      Expiry status
-----
-----
-----
10.17.65.115   sree_sc_65_115  master/ conductor  8.2.0.0-mm-dev_0000
ssetty26_new  REENROLLED 2021-08-02 06:02:30  EXPIRING SOON
10.17.65.116   sree_vmc         MD        8.2.0.0-mm-dev_0000  ssetty26
REENROLLED 2021-08-02 09:54:34  EXPIRING SOON
10.17.41.82    sree_41_82      MD        8.2.0.0-mm-dev_0000  ssetty26
REENROLLED 2021-08-02 08:26:00  EXPIRING SOON
10.17.65.117   sree_65_117     standby  8.2.0.0-mm-dev_0000  ssetty26_new
REENROLLED 2021-08-02 12:57:05  EXPIRING SOON
10.17.60.120   midhavmc60.120 MD        8.2.0.0-mm-dev_0000  N/A
N/A           N/A             N/A
Total Switches: 5
```

The output of this command includes the following information:

Column	Description
IP Address	IP address of the managed device.
Name	Name of the managed device or switch.
Type	Type of device.

Column	Description
Version	Version of the ArubaOS software running on the device.
Profile	Denotes the EST profile configured on the device.
Status	The status of the EST profile.
Expiry Time	Denotes the date and time of the expiry of the certificate enrollment.
Expiry Status	Denotes the current expiry status such as Certificate is Expiring Soon, Expired, or Not Expired.

Command History

Version	Description
ArubaOS 8.8.0.0	Added a new subparameter, <code>CSR attribute Config</code> , in the output table.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show est profile

```
show est profile {default|<profile-name>}
```

Description

Displays the information of the activated EST profiles on the device. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	Name of this instance of the profile.

Example

The output of this command shows the default EST profile of a single managed device:

```
(host) [mynode] # show est profile default
EST Profile "default"
-----
Parameter                Value
-----
Server Host                N/A
Server Port                443
Challenge password        N/A
Arbitrary label            N/A
Server's CA Cert Name     N/A
Organizational Unit Name  N/A
Arbitrary enrollment label /ca:7
Arbitrary reenrollment label /ca:7
Username                   N/A
Password                   N/A
```

Related Commands

Platforms	Licensing
est	This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment.
est-activate	This command is used to activate an existing EST profile on the controller or the AP.

Command History

Version	Description
ArubaOS 8.6.0.0	The following parameters were introduced, <ul style="list-style-type: none">■Arbitraty label enrolment■Arbitrart label reenrolment■ Organizational unit name■ Username/password
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show est status

```
show est status [all]
```

Description

Displays the information of the activated EST profiles along with the current status of the EST information on the device.

Parameter	Description
all	Displays the activated EST profiles and the current status of the EST related information of the all switches.

Example

- `show est status`—Use this command to view the current status of the EST related information on the device.
- `show est status all`—Use this command to view the current status of the EST related information of all the switches.

The output of this command shows the current EST status of a single managed device:

```
(host) [mynode] # show est status
EST STATUS
-----
Profile Name       : ssetty26_new
Server Host       : 10.20.21.26
Server Port       : 8443
Enrollment status : Re-enrolled
Arbitrary label enrollment : /ca:7
Arbitrary label reenrollment : /ca:7
Expiry status     : EXPIRING SOON
Valid from        : 2017-08-01 06:02:30
Valid till        : 2017-08-02 06:02:30
Re-enrollment due : 2017-08-02 00:02:30
```

The output of this command shows the current EST status of all the switches:

```
(host) [mynode] # show est status all
EST Status for All Switches
-----
IP Address   Name           Type      Version      Profile
Status       Expiry time    Expiry status
-----
-----
```

```

10.17.65.115 sree_sc_65_115 master 8.2.0.0-mm-dev_0000 ssetty26_new
REENROLLED 2017-08-02 06:02:30 EXPIRING SOON
10.17.65.116 sree_vmc MD 8.2.0.0-mm-dev_0000 ssetty26
REENROLLED 2017-08-02 09:54:34 EXPIRING SOON
10.17.41.82 sree_41_82 MD 8.2.0.0-mm-dev_0000 ssetty26
REENROLLED 2017-08-02 08:26:00 EXPIRING SOON
10.17.65.117 sree_65_117 standby 8.2.0.0-mm-dev_0000 ssetty26_new
REENROLLED 2017-08-02 12:57:05 EXPIRING SOON
10.17.60.120 midhavmc60.120 MD 8.2.0.0-mm-dev_0000 N/A
N/A N/A N/A
Total Switches:5

```

The output of this command includes the following information:

Column	Description
IP Address	IP address of the managed device.
Name	Name of the managed device or switch.
Type	Type of device
Version	Version of the ArubaOS software running on the device.
Profile	Denotes the EST profile configured on the device.
Status	The status of the EST profile
Expiry Time	Denotes the date and time of the expiry of the certificate enrollment.
Expiry Status	Denotes the current expiry status such as Certificate is Expiring Soon, Expired, or Not Expired.

Related Commands

Platforms	Licensing
est	This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment.
est-activate	This command is used to activate an existing EST profile on the controller or the AP.

Command History

Version	Description
ArubaOS 8.6.0.0	The following parameters were introduced, <ul style="list-style-type: none"> ▪ Arbitrary label enrolment ▪ Arbitrary label reenrolment ▪ Organizational unit name ▪ Username/password
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show fake-ade-cnt

show fake-ade-cnt

Description

Display the global and current fake ade counters

Syntax

None.

Example

The following example shows the output of `show fake-ade-cnt`.

```
(host) [mynode] (config) #show fake-ade-cnt
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show fault

```
show fault [history]
```

Description

Display a list of faults, which are any problematic conditions of the ArubaOS software or hardware.

Syntax

Parameter	Description
history	Include this parameter to display a history of faults cleared by the managed device or the operator.

Usage Guidelines

A managed device can maintain a list of up to 100 faults. Once 100 faults have been logged, any faults arising after that are dropped. The managed device maintains a history of the last 100 faults that have cleared. Every time a new fault clears clear, the oldest fault in the fault history is purged from the list.

Example

This example below shows all active faults the managed device, including the time the fault occurred, the fault ID number, and a description of the problem.

```
(host) [mynode] (config) #show fault

Active Faults
-----
Time                Number  Description
----                -
2009-03-02 18:13:08  93     Authentication Server vortex is down.
2009-03-02 18:13:08  94     Authentication Server vortex is down.
2009-03-02 18:13:08  95     Authentication Server vortex is down.
2009-03-02 18:13:08  96     Authentication Server vortex is down.
2009-03-02 18:13:08  97     Authentication Server corpl-supersvr is down.
2009-03-02 18:13:08  98     All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:08  99     Authentication Server corpl-supersvr is down.
2009-03-02 18:13:08  100    All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:08  101    Authentication Server corpl-supersvr is down.
```

```

2009-03-02 18:13:08 102      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:08 103      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:08 104      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:08 105      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:08 106      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:09 107      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:09 108      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:09 109      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:09 110      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:09 111      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:09 112      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:09 113      Authentication Server corpl-supersvr is down.
2009-03-02 18:13:09 114      All authentication servers in server group sg-
auth2 are brought back in service.
2009-03-02 18:13:09 115      Authentication Server corpl-supersvr is down.
Total number of entries in the queue      :23

```

Related Commands

Command	Description
clear	Manually clear a single fault by specifying the fault ID number, or clear all faults by including the <code>all</code> parameter.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on managed devices.

show file syncing profile

show file syncing profile

Description

This command displays the configuration the file syncing profile.

Syntax

None.

Usage Guidelines

Execute this command to view the file syncing profile.

Example

The following example shows the output of `show file syncing profile`.

```
(host) [mynode] (config) #show file syncing profile
File syncing profile
-----
Parameter      Value
-----
File syncing    Enabled
sync time      30
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licenses	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show fips

show fips



This command applies only to the FIPS version of ArubaOS.

Description

Displays FIPS mode of operation status as enabled or disabled.

Syntax

No parameters.

Example

The output of this command shows that the FIPS mode of operation is currently enabled.

```
(host) [mynode] (config) # show fips  
  
FIPS Settings:  
-----  
Mode   Enabled
```

Related Commands

Command	Description
fips	This command enables and disables the FIPS mode of operation.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and managed devices.

show firewall

```
show firewall [debug-route][dns-names]
```

Description

Display a list of global firewall policies and policy details.

Syntax

Parameter	Description
debug-route	Show global route debug settings, including the route protocol (IPv4/IPv6) and IP address.
dns-names	Display a list of DNS names and IP addresses used in firewall commands.

Examples

Include the optional `dns-names` parameter to list the DNS names used in firewall policies currently configured on the controller.

```
(host) [mynode] #show firewall dns-names
FW DNS names
-----
Name                Id  InUse  List
-----
*.google.           13  1      216.58.213.174 216.58.213.163
74.125.24.94 216.58.210.131
youtube.googleapis.com  9  1
m.youtube.com       7  1
accounts.google.com  1  1
www.youtube.com     6  1      64.233.167.91 64.233.167.93
64.233.167.190 216.58.198.110
graph.facebook.com  3  1
www.bing.com        12  1      204.79.197.200
www.youtube-nocookie.com 10  1
ssl.gstatic.com     2  1      216.58.213.163 216.58.198.99
youtubei.googleapis.com  8  1
www.googleapis.com  11  1      216.58.213.138 64.233.184.95
facebook.com        5  1
fbstatic-a.akamaihd.net 4  1
```

This example shows if DPI classification is enabled or disabled:


```
(host) [mynode] #show firewall | include DPI
DPI Classification           Disabled [Cfg: disabled, PEF 1
License: installed]
DPI classification cache    Enabled
```

This example below shows all firewall policies currently configured on the controller.

```
(host) [mynode] #show firewall
Global firewall policies
-----
Policy                               Action      Rate      Port
-----
Enforce TCP handshake before allowing data  Disabled
Prohibit RST replay attack                 Disabled
Deny all IP fragments                      Disabled
Prohibit IP Spoofing                       Enabled
Monitor ping attack                         Disabled
Monitor TCP SYN attack                     Disabled
Monitor IP sessions attack                 Disabled
Deny inter user bridging                   Disabled
Log all received ICMP errors               Disabled
Per-packet logging                         Disabled
Blacklist/Denylist Grat ARP attack client  Disabled
Allow tri-session with DNAT                Disabled
Disable FTP server                          No
Blacklist/Denylist ARP attack client       Disabled
Monitor ARP attack                         Disabled
Monitor Gratuitous ARP attack              Enabled   50/30sec
GRE call id processing                     Disabled
Session Idle Timeout                       Enabled   16 sec
WMM content enforcement                    Disabled
Trust packet QoS                           Disabled
Only allow local subnets in user table    Disabled
Monitor/police CP attacks                  Disabled
Rate limit CP untrusted ucast traffic      Enabled   9765 pps
Rate limit CP untrusted mcast traffic      Enabled   3906 pps
Rate limit CP trusted ucast traffic        Enabled   65535 pps
Rate limit CP trusted mcast traffic        Enabled   3906 pps
Rate limit CP route traffic                Enabled   976 pps
Rate limit CP session mirror traffic       Enabled   976 pps
Rate limit CP auth process traffic         Enabled   976 pps
Rate limit CP vrrp traffic                 Enabled   512 pps
Rate limit CP ARP traffic                  Enabled   3906 pps
Rate limit CP L2 protocol/other traffic    Enabled   1953 pps
Deny inter user traffic                    Disabled
Prohibit ARP Spoofing                      Disabled
Enforce bw contracts for broadcast traffic  Disabled
Multicast automatic shaping                Disabled
Stall Detection                            Disabled
Enforce TCP Sequence numbers               Disabled
AMSDU Rx                                   Enabled
Jumbo Frames                               Disabled
Session-tunnel FIB                         Enabled
Prevent DHCP exhaustion                    Disabled
```

```

Deny source routing                Disabled
Immediate Freeback                 Disabled
Stateful ICMP Processing            Disabled
Optimize Duplicate Address Detection frames Enabled
Mcast RED                          Disabled
IPSec Mark Management Frames        Disabled
Rate limit CP IP Error pkts         Enabled    128 pps
Wireless Bridge Aging              Enabled
Port Packet Drop Log Enable         Disabled
App performance monitoring           Disabled
DHCP performance monitoring          Disabled
Drop Larger than GRE MTU DF frame, send ICMP Err Disabled
Drop Larger than GRE MTU DF frame   Disabled
Drop Larger than GRE MTU frame, send ICMP Err Disabled
Drop Larger than GRE MTU frame      Disabled
Enable GRE Inner Frame Fragmentation Disabled
Drop Larger than IPSEC MTU DF frame Enabled
Track Spoofs in Data Path           Disabled
Rate limit CP IKE traffic            Disabled
High Water Mark Percent for Outstanding Buffers Disabled
Monitoring Frequency for Outstanding Buffers Disabled
DPI classification cache             Enabled
Drop all ip spoofs                  Disabled
Prohibit RC Update                  Disabled
Enable session-spread               Disabled

```

The output of this command includes the following information:

Parameter	Description
Enforce TCP handshake before allowing data	If enabled, this feature prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.
Prohibit RST replay attack	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.
Deny all IP Fragments	If enabled, all IP fragments are dropped.

Parameter	Description
Prohibit IP Spoofing	When this option is enabled, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
Monitor ping attack	If enabled, the controller monitors the number of ICMP pings per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor TCP SYN attack	If enabled, the controller monitors the number of TCP SYN messages per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor IP sessions attack	If enabled, the controller monitors the number of TCP sessions requests per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack sessions.
Deny inter user bridging	If enabled this setting prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
Enable GRE Inner Frame Fragmentation	If enabled, the inner GRE frames are fragmented, when packet length is greater than tunnel MTU.
Drop Larger than GRE MTU DF frame, send ICMP Err	If enabled, IP packets with DF bit set are dropped when packet length is greater than GRE tunnel MTU and an ICMP error message is sent.
Drop Larger than GRE MTU DF frame	If enabled, IP packets with DF bit set are dropped when packet length is greater than GRE tunnel MTU and an ICMP error message is not sent.

Parameter	Description
Drop Larger than GRE MTU frame, send ICMP Err	If enabled, IP packets are dropped when packet length is greater than GRE tunnel MTU and an ICMP error message is sent.
Drop Larger than GRE MTU frame	If enabled, IP packets are dropped when packet length is greater than GRE tunnel MTU and an ICMP error message is not sent.
Log all received ICMP errors	Shows if the controller will log received ICMP errors.
Per-packet logging	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.
Blacklist/Denylist Grat ARP attack client	If enabled, blacklist/denylistclients exceeding the Gratuitous ARP attack rate.
Allow tri-session with DNAT	Shows if the controller allows three-way session when performing destination NAT.
Disable FTP server	If active, this feature disables the FTP server on the controller.
Blacklist/Denylist ARP attack client	If enabled, blacklist/denylistclients exceeding the ARP attack rate.
Monitor ARP attack	Shows the status of the ARP attack monitor.
Monitor Gratuitous ARP attack	Shows the status of the Gratuitous ARP attack monitor.
GRE call id processing	If active the controller creates a unique state for each PPTP tunnel.
Session Idle Timeout	Shows if a session idle timeout interval has been defined.
WMM content enforcement	If traffic to or from the user is inconsistent with the associated QoS policy for voice, this feature reclassifies traffic to best effort and data path counters are incremented.

Parameter	Description
Session VOIP Timeout	If enabled, a idle session timeout is defined for sessions that are marked as voice sessions.
Trust packet QoS	Displays if the RTP traffic is passed without changing the DSCP value.
Only allow local subnets in user table	If enabled, the controller only adds IP addresses which belong to a local subnet to the user table.
Monitor/police CP attacks	If enabled, the controller monitors a misbehaving user's inbound traffic rate. If this rate is exceeded, the controller can register a denial of service attack.
Rate limit CP untrusted ucast traffic	Shows the inbound traffic rate
Rate limit CP untrusted mcast traffic	Displays the untrusted multicast traffic rate limit.
Rate limit CP trusted ucast traffic	Displays the trusted unicast traffic rate limit.
Rate limit CP trusted mcast traffic	Displays the trusted multicast traffic rate limit.
Rate limit CP route traffic	Displays the traffic rate limit for traffic that needs generated ARP requests.
Rate limit CP session mirror traffic	Displays the traffic rate limit for session mirrored traffic forwarded to the controller.
Rate limit CP auth process traffic	Displays the traffic rate limit for traffic forwarded to the authentication process.
Rate limit CP vrrp traffic	Displays the rate limit of VRRP traffic routed to the control plane.
Rate limit CP ARP traffic	Displays the ARP traffic rate limit in packets per second.
Rate limit CP L2 protocol/other traffic	Displays the traffic rate limit for L2 protocol and L2 special handling traffic.

Parameter	Description
Rate limit CP IP Error pkts	Displays the rate limit error IP in packets per-second.
Rate limit CP IKE traffic	Displays the traffic rate limit from IKE to CP, in packets per second.
Deny inter user traffic	If enabled, this setting disables traffic between all untrusted users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
Prohibit ARP Spoofing	When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.
Enforce bw contracts for broadcast traffic	If enabled, bw contracts are applied ot local subnet broadcast traffic.
Multicast automatic shaping	If enabled, enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.
Stall Detection	If enabled, triggers datapath crash on stall detection. Applies to the to 7200 Seriescontrollers only.
Enforce TCP Sequence numbers	If enabled, prevents data from passing between two clients until the three-way TCP handshake has been performed.
AMSDU Rx	AMSDU packets are dropped if this option is enabled.
Jumbo Frames	If enabled, supports up to 9216 bytes of payload on the controller.
Session-tunnel FIB	Enables session tunnel based forwarding.

Parameter	Description
Prevent DHCP Exhaustion	If enabled, this option checks for DHCP client hardware address against the packet source MAC address. This command checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. This feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.
Deny Source Routing	If enabled, forwarding of IP frames with source routing with the source routing options set is disallowed.
Immediate Freeback	If enabled, immediately frees buffers on 7200 Series controllers. Do not enable this option unless instructed to do so by a technical support representative.
DPI Classification	If enabled, performs deep packet inspection.
Track Spoofs in Data Path	If enabled, checks if there is a spoof in datapath.
Web Content Classification	If enabled, allows web content classification for all HTTP traffic. Default: disabled
Web Content Cache Miss Drop	If enabled, allows the controller to drop any packets that do not match any web content category or reputation levels in the controller's internal web content cache. Default: disabled
Optimize Duplicate Address Detection frames	Reduce flooding of IPv4 Gratuitous ARPs/IPv6 Duplicate Address Detection frames onto wireless clients. Default: enabled

Related Commands

Command	Description
firewall	This command configures firewall options on the controller.
firewall cp	This command creates whitelist/allowlist session ACLs
firewall cp-bandwidth-contract	This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.

Command History

Version	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> . All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.8.0.0	The output was modified to include the DPI classifications.
ArubaOS 8.7.0.0	The output was modified to include the following parameters: <ul style="list-style-type: none"> ▪ <code>Enable GRE Inner Frame Fragmentation</code> ▪ <code>Drop Larger than GRE MTU DF frame, send ICMP Err</code> ▪ <code>Drop Larger than GRE MTU DF frame</code> ▪ <code>Drop Larger than GRE MTU frame, send ICMP Err</code> ▪ <code>Drop Larger than GRE MTU frame</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show firewall-cp

```
show firewall-cp
  internal
```

Description

Displays the Control Path firewall policies on the controller.

Example

The output of this command shows the CP firewall policies.

```
(host) [mynode] #show firewall-cp

CP firewall policies
-----
IP Version  Source IP      Source Mask  Protocol  Start Port  End Port
Permit/Deny hits  contract
-----
-----
ipv4        any            0            6         21          21         Permit
0          test
ipv4        10.10.10.10   2.2.2.2     6         8           9         Permit
0
ipv4        2:2:2:2::2    0            1         1           2         Permit
0
```

Related Commands

Command	Description
firewall	This command configures firewall options on the controller.
firewall cp-bandwidth-contract	This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show firewall-visibility

```
show firewall-visibility {aggregate-sessions-central|debug|status}
```

Description

This command displays the policy enforcement firewall visibility process state and status information.

Parameter	Description
aggregate-sessions-central	Display firewall visibility aggregate sessions table for Aruba Central.
debug	Displays process state information for debugging firewall visibility.
status	Displays the status of firewall visibility as enabled or disabled.

Example

The following command displays the status of firewall visibility.

```
(host) [mynode] #show firewall-visibility status
enabled
```

The following command displays the status of firewall visibility sessions and their grouping based on the BSSID.

```
(host) [mynode] #show firewall-visibility status
Firewall Visibility Status:
enabled
Sort by Bssid Status:
  sorting enabled:  Enabled
  sort by bssid needed:  Enabled
```

Related Commands

Command	Description
firewall	This command configures firewall options on the controller.
firewall cp	This command creates whitelist/allowlist session ACLs
firewall cp-bandwidth-contract	This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.

Command History

Release	Modification
ArubaOS 8.10.0.0	The show firewall-visibility status command output includes the Sort by Bssid Status parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show flush-r1-on-new-r0

```
ap·flush-r1-on-new-r0 {enable|disable}
```

Description

Use this command to view the status of flushing r1 keys on new r0.

Syntax

No parameters.

Example

The following example displays the status of flushing r1 keys on new r0:

```
(host) [mynode] (config) #show flush-r1-on-new-r0
Fast Roaming flush-r1-on-new-r0:enable
```

Related Commands

Command	Description
ap flush-r1-on-new-r0	This command enables or disables flushing of R1 keys, when R0 is updated for d-tunnel or bridge mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode or Config mode.

show gap-debug

show gap-debug

Description

Displays the troubleshooting information for the global AP database.

Usage Guidelines

Use this command to identify any issues with the global AP database. This command displays the troubleshooting information for the global AP database.

Example

The following is a sample output of this command:

```
(host) [mynode] (6000-202) #show gap-debug
GAP Master/Conductor LMS Table
-----
IP           Master/Conductor Cookie           Master/Conductor Seq  LMS
Cookie      LMS Seq  Activity  Status  Msg In Prog  Msg Len  Attempts
Last Reset Reason
--          -
-----
172.20.1.101 172.20.1.102,521bbce7 0 0 0.0.0.0,00000000 0
--          up      no      -      -      down notification
172.20.1.102 172.20.1.102,521ba3b1 0 0 0.0.0.0,00000000 0
--          up      no      -      -      switched to backup
192.168.2.2  172.20.1.102,521ba5e6 0 0 192.168.2.2,521ba6fd 170
30          up      no      -      -      down notification
192.168.3.2  172.20.1.102,521ba67e 0 0 192.168.3.2,521ba71b 172
34          up      no      -      -      down notification
192.168.4.2  172.20.1.102,521ba6af 0 0 192.168.4.2,521ba724 163
58          up      no      -      -      down notification
192.168.5.2  172.20.1.102,521ba6be 0 0 192.168.5.2,521ba794 169
19          up      no      -      -      down notification
192.168.6.2  172.20.1.102,521ba694 0 0 192.168.6.2,521ba730 163
40          up      no      -      -      down notification
192.168.7.2  172.20.1.102,521ba677 0 0 192.168.7.2,521ba6fd 170
29          up      no      -      -      down notification
```

The output of this command includes the following information:

Parameter	Description
IP	The IP address of the managed device

Parameter	Description
Master/Conductor Cookie	The cookie information on Mobility Conductor that is used to communicate with the LMS.
Master/Conductor Seq	The sequence number used by Mobility Conductor to sync up with the LMS. This tracks the number of times Mobility Conductor has communicated with the LMS.
LMS Cookies	The cookie information on the LMS that is used to communicate with Mobility Conductor.
LMS Seq	The sequence number used by the LMS to sync up with Mobility Conductor. This tracks the number of times the LMS has communicated with Mobility Conductor.
Activity	The time at which the last activity happened on the LMS.
Status	Indicates if the status of the LMS is up or down.
Msg in Prog	Indicates if an active communication is happening between the LMS and Mobility Conductor. It can be Yes or No. If it is yes, then the Msg Len and Attempt fields are set.
Msg Len	The length of the message that Mobility Conductor is syncing with the LMS.
Attempts	Number of times Mobility Conductor has attempted to sync with the LMS.
Last Reset Reason	Indicates the reason for last reset.

Related Commands

Command	Description
<code>ap gap-db</code>	Resynchronize an AP status on a managed device and Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show gateway health-check

show gateway health-check

Description

Display the current status of the gateway health-check feature.

Syntax

No parameters.

Usage Guidelines

The gateway health check feature can only be enabled by Aruba Technical Support.

Example

This example below shows that the gateway health-check feature has not been enabled on the managed device.

```
(host) [mynode] (config) #show gateway health-check
Gateway health check not enabled
```

Related Commands

Command	Description
gateway health-check	Disable the gateway health check

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show global-user-table

Syntax

```
show global-user-table count|list
```

Description

This command displays a count of global user based on the specified criteria or displays the list of users matching the given criteria.

Parameter	Description
count	Show the number of users matching the given criteria
ap-name	Count users matching the specified AP name
authentication-method	Count users matching the specified authentication method
bssid	Count users matching the specified BSSID
current-switch	Match IP address of the switch where the user is currently associated
ssid	Count users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
phy-type	Count users matching the specified Phy type
role	Count users matching the specified role
age	Count users matching the specified age
list	Show users matching the given criteria
ap-name	Lists users matching the specified AP name
authentication-method	Lists the users matching the specified authentication method
bssid	Lists the users matching the specified BSSID
current-switch	Match IP address of the switch where the user is currently associated
current-switch-v6	Match IPv6 address of the switch where the user is currently associated

Parameter	Description
devtype	Lists the users matching device type
ssid	Lists the users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
ip	Match IP address
ipv6	Match IPv6 address
mac-addr	Match MAC address
name	Match name
not	Show users that do not satisfy the given criteria
or	Show users that satisfy any of the given condition
phy-type	Match PHY type
role	Match role
rows	Show certain rows
start	Show user table starting from the specific row

Examples

```
(host) [mynode] #show global-user-table list

Global Users
-----
      IP          MAC          Name      Current switch  Role  Auth  AP name
Roaming  Essid    Bssid  Phy  Profile  Type  User Type
-----
--
-----

Total entries = 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show gsm

```
show gsm
  application
  channel-matrix
  debug
  lookup
```

Description

This command displays the list of all interfaces. Click the parameter links below to view the corresponding show commands.

Parameter	Description
application	Displays the status of the GSM application, for example, stm, auth, and so on.
channel-matrix	Displays the channels with Publisher and Subscriber Information.
debug	Displays status, event ring channel information, and trace events for channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on.
lookup	Displays status, event ring channel information, and trace events for specific channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show gsm application

show gsm application <application_name> status

Description

Displays the status of the GSM application, for example, stm, auth, and so on.

Parameter	Description
<application_name>	GSM application name like stm, auth, and so on.

Example

The following is a sample output of this command:

```
(host) [mynode] (config) #show gsm application stm status
GSM Tick(500 us/tick, gsm_tick=2932440723368, gsm_ticktime=1466220361684074)
Application Histogram:stm

+-----+-----+-----+-----+-----+
+-----+
|          Histogram| GSM Thread|   GSM Thread|   GSM Thread|   Main
Thread|   Main Thread|
|Time Range (in ms)| Cycle Time|API Mutex Wait|API Mutex Hold|API Mutex
Wait|API Mutex Hold|
+-----+-----+-----+-----+-----+
+-----+
| 0.000 ..   0.500|          14|          14|          14|
2477350|          2477266|
| 0.500 ..   1.000|           0|           0|           0|
0|           25|
| 1.0 ..     2.0|           1|           0|           0|
0|           43|
| 2.0 ..     4.0|           0|           0|           0|
0|           14|
| 4.0 ..     8.0|           0|           0|           0|
0|            1|
| 8.0 ..    16.0|           0|           0|           0|
0|            1|
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show gsm channel-matrix

show gsm channel-matrix

Description

Displays the channels with Publisher and Subscriber Information.

Example

The following is a sample output of this command:

```
(host) [mynode] (config) #show gsm channel-matrix
GSM Channel Matrix
-----
Channel                Publishers                Subscribers
-----                -
ap                      air_group arm dds ucm
nbapi
bss                     auth air_group arm dds
ucm

radio                  air_group arm dds ucm
nbapi

sta                    auth arm dds ucm nbapi_
help

mac_user              auth air_group dds ucm
nbapi_helper_proc
ip_user               auth air_group dds ucm
nbapi_helper_proc
user                  auth air_group dds ucm
nbapi_helper_proc
wired_ap              dds

ag_user

dev_id_cache          arm dds nbapi_helper_
proc
sectun                ha_mgr cfgm sc_replication_mgr dds ipstm appRF

key_cache             air_group dds

pmk_cache
```

```

rep_key          ipstm ha_mgr sc_replication_mgr dds
port_info        fpapps                                dds
lldp_info        fpapps
lldp_chassis_info fpapps
dds_peer         dds                                auth ucm
ucc_client       ucm                                stm
ucc_session      ucm                                stm arm
vlan_info        fpapps                                air_group dds

```

```

Multi
helper_proc mcell          writer Is Replicated
nbapi_helper_procmcell No
helper_proc mcell          Yes
er_proc      mcell          Yes
No
No
No
No
No
No
No
Yes
No
No
Yes
No
No
No
No
No
No
No
Yes

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show gsm debug

```
show gsm debug
channel
  ag_user
  ale_sta
  all
  amon_registration
  ap
  application_status
  blacklist/denylist
  bss
  bucket_map
  cac_usage
  cluster
  cluster_aac
  cluster_ap
  cluster_bss
  cluster_sta
  cluster_tunneled_node
  dds_peer
  dev_id_cache
  device_config
  device_lclist
  ha_info
  ip_probe
  ip_user
  ipsec_tunnel_info
  key_cache
  license_keys
  lldp_chassis_info
  lldp_info
  mac_user
  mip_proxy
  mip_tunnel
  named_vlan_info
  pmk_cache
  port_info
  radio
  rap_whitelist/rap_allowlist
  remote_ip_user
  rep_key
  sectun
  service_ctrl_info
  sta
  sys_racl
  tunneled_node
  tunneled_user
  ucc_client
  ucc_session
  user
  v4_dhcp_pool
  via_user
  vlan_info
```

```
web_cc_info
wired_ap
rkey
assignment
```

Description

This command displays status, event ring channel information, and trace events for channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on.

Parameter	Description
Channel	Channel Name
ag_user	AirGroup User Channel
ale_sta	Analytics and Location Engine Data
all	All GSM Channels
amon_registration	AMON messages Registration Data
ap	AP Channel
application_status	Application Status Data
blacklist/denylist	Blacklist/Denylist Channel
bss	BSS Channel
bucket_map	STA Hash Bucket to UAC map
cac_usage	Call Admission Control Usage Data
cluster	controller Cluster Info
cluster_aac	Cluster AAC Assignment Data
cluster_ap	Cluster AP Data
cluster_bss	Cluster BSS Data
cluster_sta	Cluster STA Data
cluster_tunneled_node	Cluster Tunneled Node Channel.
dds_peer	DDS Peer Info
dev_id_cache	Device Id Cache Channel
device_config	Device Config

Parameter	Description
device_lclist	Device Lclist
dhcpd_via_info	DHCP VIA Channel
ha_info	HA Info Channel
ip_probe	MIP Proxy Info
ip_user	IP User Channel
ipsec_tunnel_info	ipsec_tunnel_info Channel
key_cache	Key Cache Channel
license_keys	License Keys Channel
lldp_chassis_info	LLDP Chassis Info Channel
lldp_info	LLDP Info Channel
mac_user	Layer 2 MAC user Channel
mip_proxy	MIP Proxy Info
mip_tunnel	Mobileip tunnel control information.
named_vlan_info	Named vlans information.
pmk_cache	PMK Cache Channel
port_info	Port Info Channel
radio	Radio Channel
rap_whitelist/rap_allowlist	RAP Whitelist/Allowlist Channel
remote_ip_user	Remote IP User Data
rep_key	Replication Key Channel
sectun	Secured Tunnel Channel
service_ctrl_info	Service Control Info
sta	STA Channel
sys_racl	sys_racl Data
tunneled_node	Tunneled Node Channel.
tunneled_user	Tunneled User Channel.

Parameter	Description
ucc_client	UCC Client Channel
ucc_session	UCC Session Channel
user	User Channel
v4_dhcp_pool	v4 DHCP Pool Info
via_user	VIA VPN users information
vlan_info	VLAN Info Channel
web_cc_info	Web content classification Info Channel
wired_ap	Wired AP Channel
rkey	Replication key
assignment	Current Replication Key assignment
rap_public_ip	Displays the public IP address of the Remote AP cluster configured behind NAT.

Example

The following command checks the status of the tunneled node:

```
(host) [mynode] #show gsm debug channel tunneled_node status
GSM Channel status for Channel:TUNNELED_NODE
CSM:: Key = 0X1BB7, Size = 357612 B
DSM:: Base Key = 0X1BB8, Size = 524288 B Max number of segments = 1 Segments
created = 1
DSM:: In current segment: free_slots = 3040
Object Size = 165 B, Key Size = 6 B
Max number of Objects = 2048
Number of Allocated Objects = 0
Number of Objects in use = 0
Producers of TUNNELED_NODE channel are
tunneled_node_mgr
Subscribers of TUNNELED_NODE channel are ---
stm
cluster_mgr
The following command checks the status of the cluster:
(host) [mynode] #show gsm debug channel cluster
cluster Channel Table
-----
state v_repkey controller_ip controller_mac cluster_name cluster_redundancy
cluster_priority
cluster_connected cluster_leader cluster_role rep_key mcast_vlan cluster_vip
cluster_ap_limit
```

```

cluster_sta_limit ap_load_balancing rap_public_ip dual_controller_ip
-----
-----
-----
-----
ACTV 3 2001:1017:6181::84 00:1a:1e:04:b2:48 mixmode_clusterv6 1 128 1 0 1
4294967295 0 0.0.0.0
0 0 1 0.0.0.0 10.17.61.84 ACTV 4294967295 2001:1017:6181::85
00:00:00:00:00:00 mixmode_
clusterv6 1 128 1 1 0 8 0 0.0.0.0 0 0 1 0.0.0.0 10.17.61.85
Total Num of Objects :2
Total Num of Active Objects :2
Total Num of Replicated Objects :0

```

Command History

Release	Modification
ArubaOS 8.9.0.0	The following parameters have been modified: <ul style="list-style-type: none"> ■All instances of <code>blacklist</code> were replaced by <code>denylist</code>. ■All instances of <code>rap_whitelist</code> were replaced by <code>rap_allowlist</code>.
ArubaOS 8.8.0.0	The output of the <code>show gsm debug channel</code> command was modified to include <code>dhcpd_via_info</code> parameter.
ArubaOS 8.7.0.0	The output of the <code>show gsm debug channel cluster</code> command was modified to include <code>dual_controller_ip</code> parameter.
ArubaOS 8.6.0.0	The <code>remote_ip_user</code> parameter was added.
ArubaOS 8.4.0.0	The <code>via_user</code> and <code>rap-public-ip</code> sub-parameters were added in <code><channel></code> parameter.
ArubaOS 8.2.0.0	The <code>sectun</code> parameter accepts IPv6 addresses.
ArubaOS 8.1.0.0	The <code>tunneled_node</code> and <code>tunneled_user</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show gsm lookup

```
show gsm lookup
channel
  ag_user
  ale_sta
  amon_registration
  ap
  application_status
  blacklist/denylist
  bss
  bucket_map
  ccm_state
  cluster
  cluster_aac
  cluster_ap
  cluster_bss
  cluster_sta
  cluster_tunneled_node
  dds_peer
  dev_id_cache
  device_config
  device_lclist
  device_unprov
  ha_info
  ip_probe
  ip_user
  ipsec_tunnel_info
  key_cache
  license_keys
  lldp_chassis_info
  lldp_info
  mac_user
  mip_proxy
  mip_tunnel
  named_vlan_info
  ofa_port
  pmk_cache
  port_info
  radio
  rap_whitelist/rap_allowlist
  rep_key
  sectun
  service_ctrl_info
  split_tunnel
  sta
  sys_racl
  tunneled_node
  tunneled_user
  ucc_client
  ucc_session
  user
  vlan_info
  vrrp_info
```

```
web_cc_info
wired_ap
```

Description

This command displays status, event ring channel information, and trace events for specific channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on. The optional output modifiers `| begin` , `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
Channel	Channel Name
ag_user	AirGroup User Channel
ale_sta	Analytics and Location Engine Data
amon_registration	AMON messages Registration Data
ap	AP Channel
application_status	Application Status Data
blacklist/denylist	Blacklist/Denylist Channel
bss	BSS Channel
bucket_map	STA Hash Bucket to UAC map
ccm_state	Centralized Configuration Module state
cluster	controller Cluster Info
cluster_aac	Cluster AAC Assignment Data
cluster_ap	Cluster AP Data
cluster_bss	Cluster BSS Data
cluster_sta	Cluster STA Data
cluster_tunneled_node	Cluster Tunneled Node Channel.
dds_peer	DDS Peer Info
dev_id_cache	Device Id Cache Channel
device_config	Device Config

Parameter	Description
device_lclist	Device LC list
device_unprov	Unprovisioned device
ha_info	HA Info Channel
ip_probe	MIP Proxy Info
ip_user	IP User Channel
ipsec_tunnel_info	ipsec_tunnel_info Channel
key_cache	Key Cache Channel
license_keys	License Keys Channel
lldp_chassis_info	LLDP Chassis Info Channel
lldp_info	LLDP Info Channel
mac_user	Layer 2 MAC user Channel
mip_proxy	MIP Proxy Info
mip_tunnel	Mobileip tunnel control information.
named_vlan_info	Named vlans information.
ofa_port	OpenFlow Port Channel
pmk_cache	PMK Cache Channel
port_info	Port Info Channel
radio	Radio Channel
rap_whitelist/rap_allowlist	RAP Whitelist/AllowlistChannel
rep_key	Replication Key Channel
sectun	Secured Tunnel Channel
service_ctrl_info	Service Control Info
split_tunnel	Split Tunnel
sta	STA Channel
sys_racl	sys_racl Data
tunneled_node	Tunneled Node Channel.

Parameter	Description
tunneled_user	Tunneled User Channel.
ucc_client	UCC Client Channel
ucc_session	UCC Session Channel
user	User Channel
vlan_info	VLAN Info Channel
vrrp_info	Virtual Router Redundancy Protocol Information
web_cc_info	Web content classification Info Channel
wired_ap	Wired AP Channel

Example

The following example displays the GSM channel report for a radio with BSSID 48:4a:e9:7c:8c:d0:

```
(host) [mynode] #show gsm lookup channel radio key radio_bssid
48:4a:e9:7c:8c:d0

Object details as follows:
      state      :: ACTV
      rep_key     :: 1
      v_repkey    :: 3
      radio_bssid :: 48:4a:e9:7c:8c:d0
      ap_name     :: 48:4a:e9:cf:c8:cc
      ap_ip_address :: fd8d:3da:cf00:666:828d:b7ff:fec0:fc
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> . All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.7.0.0	The output of the following commands was modified to display IPv6 address of the AP: <ul style="list-style-type: none"> ■ <code>show gsm lookup channel radio key radio_bssid <radio_bssid></code>

Release	Modification
	<ul style="list-style-type: none"> ■ <code>show gsm lookup channel sta_mac_address <sta_mac_address></code>
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show guest-access-email

show guest-access-email

Description

This command shows a guest access email profile configuration. The guest access email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the GPP.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the current guest access email profile parameters. The **Parameter** and **Value** columns show the configured SMTP server and SMTP ports. that process guest email.

```
(host) [mynode] (config) #show guest-access-email

Guest-access Email Profile
-----
Parameter      Value
-----
SMTP Server    10.1.1.4
SMTP Port      25
```

Related Commands

Command	Description
guest-access-email	This command shows a guest access email profile configuration.
local-userdb-guest add	This command creates a guest user in a local user database.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ha

```
show ha
  ap
  group-membership
  group-profile
  heartbeat counters
  oversubscription statistics
```

Description

This command displays the list of all interfaces. Click the parameter links below to view the corresponding show commands.

Parameter	Description
ap	Displays information about APs using the HA feature.
group-profile, group-membership	Displays HA profile settings and shows the HA group to which the managed device is currently assigned.
heartbeat counters	Displays statistics for the HA extended managed device capacity feature.
oversubscription statistics	Displays statistics for the HA extended managed device capacity feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable or Config mode on Mobility Conductor.

show ha ap

```
show ha ap
  information {ip-addr <ip-addr>|ip6-addr <ip6-addr>}
  table
```

Description

This command displays information about APs using the High-Availability (HA) features. The HA features work across Layer-3 networks, so there is no need for a direct Layer-2 connection between a High-Availability group when the AP first connects to its active. The active provides the IP address of a standby and the AP attempts to establish a tunnel to the standby. If an AP fails to connect to the first standby, then the active will select a new standby for that AP, and the AP will then attempt to connect to that standby .

An AP will failover to its backup if it fails to contact its active through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

Parameter	Description
<pre>information ip-addr <ip-addr> ip6-addr <ip6-addr></pre>	Issue this command under the supervision of Aruba support to troubleshoot the HA feature.
<pre>table</pre>	Display the HA AP table to view information about APs configured to use the HA feature.

Examples

The following command displays the HA table for the HA group **default**:

```
(host) [mynode] (config) #show ha ap table
HA AP Table
-----
AP          IP-Address   MAC-Address   AP-flags  HA-flags
--          -
ard         10.3.31.245  6c:f3:7f:c6:72:c0  LU
arr         10.3.31.222  d8:c7:c8:c0:02:7c  LU
kalap105-2  10.3.31.253  00:24:6c:c0:22:6b  LU          S
Total Num APs::3
Active APs::2
Standby APs::1
AP Flags: R=RAP; S=Standby; s=Bridge Split VAP L=Licensed; M=Mesh, U=Up
HA Flags: S=Standby, C=Standby connected, L=LMS, F=Sent Failover Request to
AP,
H=AP flagged for Inter Controller Heartbeat
```

Related Commands

Command	Description
ha	This command configures the High Availability: Fast Failover feature by assigning a managed device or standby controller to a High-Availability group, and defining the deployment role for each controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Conductor.

show ha group

```
show ha
  group-membership
  group-profile [<profile>]}
```

Description

This command displays HA profile settings and shows the HA group to which the managed device is currently assigned. The HA feature supports redundancy models with an active managed device pair, or an active or standby deployment model with one backup managed device supporting one or more active managed devices. Each of these clusters of active and backup managed devices comprises a HA group. Note that all active and backup managed devices within a single HA group must be deployed in a single Mobility Conductor - managed device topology. The HA feature works across Layer-3 networks, so there is no need for a direct Layer-2 connection between managed devices in a HA group.

Parameter	Description
group-membership <profile>	Name of the HA group to which the managed device should be a member.
group-profile [<profile>]	Display a list of all HA groups, or include the optional <profile> parameter to display configuration settings for the specified profile.

Examples

The following command shows that the managed device from which the command was issued is a member of the HA group ha-group2:

```
(host) [mynode] (config) #show ha-group-member
Member of HA group :ha-group2
```

The following example shows that the managed device has two configured HA group profiles. The **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column:

```
HA group information List
-----
Name      Profile Status
----      -
default
new
Total: 2
```

Related Commands

Command	Description
ha	This command configures the High Availability: Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Conductor.

show ha heartbeat counters

```
show ha heartbeat counters
```

Description

This command displays statistics for the HA extended managed device capacity feature. The HA inter-managed device heartbeat feature allows for faster AP failover from an active managed device to a standby managed device, especially in situations where the active managed device reboots or loses connectivity to the network.

The inter-managed device heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the managed device. If enabled, the inter-managed device heartbeat feature supersedes the AP's heartbeat to its managed device. As a result, if a standby managed device detects missed inter-managed device heartbeats from the active managed device, it triggers its standby APs to failover to the standby managed device, *even if those APs have not detected any missed heartbeats between the APs and their active managed device*. Use this feature with caution in deployments where the active and standby managed device are separated over high-latency WAN links.

This feature is disabled by default. It can be used in conjunction with the HA state synchronization feature only in topologies that use a single active and standby managed device, or a pair of dual-mode active managed devices that act as a standby managed device for each other. HA inter-managed device heartbeats can be enabled and configured in the HA group profile using the WebUI or CLI.

Examples

The following command displays HA heartbeat statistics for the HA group **default**:

```
(host) [mynode] (HA group information "default") #show ha heartbeat counters

Heartbeat stats
-----
Controller IP   Active Reference Count      Total Heartbeat Sent      Total
Heartbeat Received
-----
-----
172.14.0.2      1                          101                        101

Last Missed Heartbeat (Count) Time
-----
0
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the managed device from which this command was issued.
Active Reference Count	Number of APs that are using that standby managed device as their active managed device.
Total HeartBeat Sent	Total number of heartbeats sent by the managed device.
Total Heartbeat REceived	Total number of heartbeats received by the managed device.
Last Missed Heartbeat(count) time	Timestamp showing when the last heartbeat sent was not received, as well as the number of heartbeats that failed to be sent.

Related Commands

Command	Description
ha	This command configures the High Availability: Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Conductor.

show ha oversubscription statistics

show ha oversubscription statistics

Description

This command displays statistics for the HA extended managed device capacity feature. A managed device acting as a standby managed device can oversubscribe to standby APs by up to four times that managed device's rated AP capacity, as long as the tunnels consumed the standby APs do not exceed the maximum tunnel capacity for that standby managed device.

Feature Requirements

All managed devices using this feature must be deployed in a master/ conductor -local topology where centralized licensing is enabled on the active and standby managed device. If centralized licensing is disabled, the standby AP oversubscription feature is also disabled. Standby managed device oversubscription and the HA state synchronization features are mutually incompatible and cannot be enabled simultaneously. If your deployment uses the state synchronization feature, you must disable it before you enable standby managed device oversubscription.

Standby Managed Devices Capacity

The following table describes the AP oversubscription capacity maximum supported tunnels and for managed devices that support this feature:

controller Model	Standby AP Capacity	Maximum Tunnels Supported
7210	4x rated AP capacity	16384 tunnels
7220	4x rated AP capacity	32768 tunnels
7240	4x rated AP capacity	65536 tunnels

To determine the number of standby tunnels consumed by APs on each active managed device, multiply the number of APs on the active managed device by the number of BSSIDs per AP. As an example, consider a deployment with four active 7210 managed devices that each have 512 APs with 8 BSSIDs. The APs on each active managed device consume (512 * 8) tunnels, for a combined total of 16,384 tunnels. A single 7210 managed device using the standby managed device oversubscription feature can act as the standby managed device for all four active managed devices in this example, because this topology is within the 4x rated AP capacity limit and maximum tunnel limit for the 7210 managed device model.

If the network administrator later changed all the APs in this deployment to support 10 BSSIDs, each active managed device would use (512 * 10) tunnels, for a combined total of 20,480 tunnels

on the four active managed devices. The tunnels required by the APs on the active managed device would then exceed the maximum tunnel limit for the standby managed device, so the standby managed device can no longer support all APs on the active managed device.

AP Failover

If a standby managed device reaches its AP oversubscription capacity or exceeds its maximum BSSID limit, the standby managed device drops any subsequent standby AP connections. A dropped AP attempts to reconnect to the standby managed device, but after it exceeds the maximum number of request retries, the AP informs the active managed device that it is unable to connect to the standby managed device. The active managed device then prompts the AP to create a standby tunnel to another standby managed device, if one is configured.

If an active managed device fails, the APs on the active managed device fail over to the standby managed device. Once the standby managed device has reached its capacity for active APs, it terminates tunnels to any standby APs that controller can no longer serve. When these APs detect that there is no longer a heartbeat between the AP and the standby managed device, they notify their active managed device that they can no longer connect to the standby. The active managed device then prompts the APs to establish standby tunnels to another standby managed device, if one is configured.

Examples

The following command displays oversubscription statistics for APs and tunnels:

```
(host) [mynode] (config) #show ha oversubscription statistics
Platform oversubscription factor :          4
APs Limits
-----
APs                Number
----             -
Platform Limit     512
Current Active     2
Current Standby    694
Active remaining   0
Standby remaining  1
Maximum allowed Standby 697

BSS Limits
-----
Tunnels           Limits
-----
Maximum BSS tunnels 16384
Average BSS/AP      23
BSS tunnels in use  16360
BSS tunnels available 24
```

The output of this command includes the following parameters:

Parameter	Description
Platform limit	Maximum number of APs supported by the managed device platform.
Current Active	Number of active APs currently associated to the managed device.
Current Standby	Number of APs that are currently using the managed device as a standby managed device.
Active Remaining	Number of APs that can connect to this managed device in Active mode.
Standby Remaining	Number of APs that can connect to this managed device in Standby mode.
Maximum allowed Standby	Maximum number of Standby APs supported by the managed device.
Maximum BSS tunnels	The maximum number of BSS tunnels supported by the managed device.
Average BSS/AP	The average number of BSS tunnels per AP using the managed device as a standby managed device.
BSS tunnels in use	Number of BSS tunnels currently in use by the managed device.
BSS tunnels available	Number of BSS tunnels not currently in use by the managed device.

Related Commands

Command	Description
ha	This command configures the High Availability:Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable mode on Mobility Conductor.

show hash statistics

Show hash statistics app-name

```
aaa
ads
authmgr
certmgr
cfgm
cpsec
cts
dbsync
dhcp
esi
fpapps
httpd
ike
l2tp
licensemgr
mobileip
mon_serv
ntp
ospf
pim
pktfilter
pptp
profmgr
publisher
resolver
sapm
snmp
stm
stm-lopri
syslogd
userdb
wms
```

Description

This command displays the Inter Process Communication statistics.

Syntax

Parameter	Description
aaa	Administrator Authentication
ads	Anomaly Detection

Parameter	Description
authmgr	User Authentication
certmgr	Certificate Manager
cfgm	Config Manager
cpsec	Control-Plane Security Manager
cts	Transport Service
dbsync	Database Synchronization
dhcp	DHCP Server
esi	Server Load Balancing
fpapps	Layer 2,3 control
httpd	HTTPD
ike	IKE Daemon
l2tp	L2TP
licensemgr	License Manager
mobileip	Mobile IP
mon_serv	Mon Server
ntp	NTP Daemon
ospf	OSPF
pim	Protocol Independent Multicast
pktfilter	Packet Filter
pptp	PPTP
profmgr	Profile Manager
publisher	Publish subscribe service
resolver	Resolver
sapm	SAPM
snmp	SNMP agent
stm	Station Management

Parameter	Description
stm-lopri	Station Management Low Priority
syslogd	Syslog Manager
userdb	User Database Server
wms	Wireless Management

Example

This example shows the NTP Daemon statistics

```
(host) [mynode] (config) #show hash statistics app-name ntp
Received response from application
Hash Statistics
Size      Nodes Max-Coll Owner
23         0         0
23        266         0
23        272         0
23        272         0
23        272         0
997         0         0
23         4         0
23         0         0
23         0         0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable mode of Mobility Conductor and managed device.

show hostname

show hostname

Description

Show the hostname of the Mobility Conductor and managed device.

Syntax

No parameters.

Example

The output of this command shows the hostname configured for the controller. A hostname can contain alphanumeric characters, spaces, punctuation, and symbol characters.

```
(host) [MyNode] # show hostname  
hostname is SampleHost
```

Related Commands

Command	Description
hostname	This command configures the Mobility Conductor's hostname.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Available on Mobility Conductor and managed device.

show iap

```
show iap
  branch-stats branch-key
  detailed-table
  statistics
  subnet
  subnet-stats subnet
  subnets-summary
  table
  trusted-branch-db
```

Description

This command displays the list of all interfaces. Click the parameter links below to view the corresponding show commands.

Parameter	Description
branch-stats branch-key	Displays the statistics of an IAP VPN branch.
detailed-table	Displays the details of all the branches terminating at the managed device.
statistics	Displays the IAP VPN statistics information.
subnet	Displays the details of specific IAP subnet information.
subnet-stats subnet	Displays the statistics of an IAP VPN subnet.
subnets-summary	Displays the summary of IAP subnet information.
table	Displays the branch details connected to the managed device.
trusted-branch-db	Displays the details of IAP trusted branch database information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show iap branch-stats branch-name

```
show iap branch-stats branch-name <brName>
```

Description

Displays the details of specific statistics of an IAP VPN branch. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
branch-name <brName>	Displays specific IAP VPN branch statistics.

Example

The following command displays details of a subnet:

```
(host) [mynode] (config) #show iap branch-stats branch-name <brName>
```

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.

Command History

Release	Modification
ArubaOS 8.60.17 and 8.7.1.9	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap detailed-table

```
show iap detailed-table
  branch-key / branch-name <brkey>
  long
```

Description

Displays the details of all the branches terminating at the managed device.

Parameter	Description
branch-key / branch-name <brkey>	Key for the branch, which is unique to each branch.
long	Displays the branches connected to the managed device in detailed view.

Example

The following example shows the details of the branches connected to the controller:

```
(host) [mynode] (config) #show iap detailed-table long

          VC Name                VC MAC Address      Status   Inner IP
VC Branch Name/Key
-----
Instant-C0:8C:08 d8:c7:c8:c4:73:53 UP          1.1.1.1
2d15576901190269568c3d9837fc1b414e1b06523282805aaa
Instant-C0:8C:08 d8:c7:c8:c4:73:53 UP          1.1.1.1
2d15576901190269568c3d9837fc1b414e1b06523282805aaa
Instant-C0:8C:08 d8:c7:c8:c4:73:53 UP          1.1.1.1
2d15576901190269568c3d9837fc1b414e1b06523282805aaa

Flags      Branch (Subnet / Vlan)  BID    IP Address Range      Client Count
-----
PD2        52                      0      52.1.1.2-52.1.1.100   5
PD3        53.1.1.8/29            0      53.1.1.1-53.1.1.100  5
PC2        51                      0

Flags: P = Primary Tunnel; B = Backup Tunnel; C = Centralized; U =
Unassigned;
      D = Distributed; L = Local; 3 = Routed(L3); 2 = Bridged(L2);
```

The output of this command includes the following parameters:

Parameter	Description
VC Name	Name of Virtual managed device of the branch.
VC MAC Address	MAC address of the Virtual managed device of the branch.
Status	Current status of the branch (UP or DOWN).
Inner IP	Internal VPN IP of the branch.
VC Branch Name/Key	Key for the branch, which is unique to each branch.
Flags	This column displays any flags for the branch subnet: P = Primary Tunnel B = Backup Tunnel C = Centralized D = Distributed L = Local U = Unassigned 3 = Routed(L3) 2 = Bridged(L2)
Branch (Subnet/Vlan)	Subnet mask or VLAN assigned to the branch.
BID	Branch ID
IP Address Range	Allocated branch subnet IP address range.
Client Count	Number of client terminating on this managed device

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following modifications were introduced: <ul style="list-style-type: none"> ▪ The output parameter, <code>Name</code> is modified as <code>VC Name</code>. ▪ The output parameter, <code>Key</code> is modified as <code>VC Branch</code>

Release	Modification
	Name.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap statistics

```
show iap statistics
```

Description

Displays the IAP VPN statistics .The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays details of a subnet:

```
(host) [mynode]#show iap statistics

IAP VPN Statistics
-----
S.No  Statistics                                     Value
----  -
1     Auth IP up Received                           0
2     Auth IP down Received                         0
3     IAP register request received from iap        0
4     IAP register request received for primary     0
5     IAP register request received for backup      0
6     IAP register request processed                0
7     IAP register request dropped                  0
8     IAP register request invalid inner ip         0
9     IAP register request trusted db verification  0
10    IAP register request branch key change        0
11    insert branch key to innerip table failed     0
12    Primary VC MAC changed                       0
13    Primary VC name changed                      0
```

```

14   New subnet added by primary           0
15   Primary requested bid different from old bid 0
16   Primary reused bid from dead branch    0
17   Primary bid allocated different from requested 0
18   Bid allocated by primary              0
.
.
.

```

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.6.0.17 and 8.7.19	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap subnet

```
show iap subnet <subnet-name>
```

Description

Displays the details of specific IAP subnet information. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
subnet <subnet-name>	Displays specific subnet information for an IAP.

Example

The following command displays details of a subnet:

```
(host) [mynode] (config) #show iap subnet test
```

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap subnet-stats subnet

```
show iap subnet-stats subnet <subnet>
```

Description

Displays the statistics of an IAP VPN subnet. The optional output modifiers | begin, | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
subnet <subnet-name>	Displays specific subnet information for an IAP.

Example

The following command displays details of a subnet:

```
(host) [mynode] (config) #show iap subnet-stats subnet <subnet>
```

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.6.0.17 and 8.7.1.9	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap subnets-summary

```
show iap subnets-summary
```

Description

Displays the summary of IAP subnet information. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays details of a subnet:

```
(host) [mynode]# show iap subnets-summary
Summary of IAP Branch Subnets
-----
S.No  Subnet Name                MaxBID  BIDs set in Bitmap  BIDs free in
Bitmap Allocated Branches      Down Branches  Reclaimed from Down Branches
-----
-----
1     1.1.1.0-1.1.1.255,1        64       4                   60
    4                        3                   0
2     50.11.0.0-50.11.255.255,5 8192     5                   8187
    5                        4                   0
3     59.59.95.0-59.59.95.100,4 12       2                   10
    2                        2                   0
```

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.6.0.17 and 8.7.1.9	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap table

```
show iap table
  branch-key <brkey>
  long
  summary
```

Description

Displays the branch details connected to the managed device.

Parameter	Description
branch-key <brkey>	Key for the branch, which is unique to each branch.
long	Displays the branches connected to the managed device in detailed view.
summary	Displays the summary of the IAP table.

Example

The following example shows the details of the branches connected to the managed device:

```
(host) [mynode] (config) #show iap table long

IAP Branch Table
-----
Assigned Subnet  VC Name      VC MAC Address  Status  Inner IP
-----
-----
Tokyo-CB:D3:16  6c:f3:7f:cc:42:f8  DOWN  0.0.0.0

Paris-CB:D3:16  6c:f3:7f:cc:3d:04  UP    10.15.207.140  10.15.206.99/29
2

LA              6c:f3:7f:cc:42:25  UP    10.15.207.111  10.15.206.24/29
2

Munich         d8:c7:c8:cb:d3:16  DOWN  0.0.0.0

London-c0:e1   6c:f3:7f:c0:e1:b1  UP    10.15.207.120  10.15.206.64/29
2

Instant-CB:D3  6c:f3:7f:cc:42:1e  DOWN  0.0.0.0

Delhi          6c:f3:7f:cc:42:ca  DOWN  0.0.0.0

Singapore     6c:f3:7f:cc:42:cb  UP    10.15.207.122  10.15.206.120/29
2

VC Branch Name/
```

```

Key          Bid(Subnet Name)
---          -
b3c65c...
b3c65c...
b3c65c...  2 (10.15.205.0-10.15.205.250, 5) , 1 (10.15.206.1-10.15.206.252, 5)
a2a65c...  0
b3c65c...  7 (10.15.205.0-10.15.205.250, 5) , 8 (10.15.206.1-10.15.206.252, 5)
b3c65c...
b3c65c...  1 (10.15.205.0-10.15.205.250, 5) , 2 (10.15.206.1-10.15.206.252, 5)
b3c65c...  14 (10.15.205.0-10.15.205.250, 5) , 15 (10.15.206.1-10.15.206.252, 5)

Total No of UP Branches      : 4
Total No of DOWN Branches   : 4
Total No of Branches        : 8

```

Tunnel End Points

The output of this command includes the following parameters:

Parameter	Description
VC Name	Name of Virtual managed device of the branch.
VC MAC Address	MAC address of the Virtual managed device of the branch.
Status	Current status of the branch (UP or DOWN).
Inner IP	Internal VPN IP of the branch.
Assigned Subnet	Subnet mask assigned to the branch.
Assigned Vlan	VLAN ID assigned to the branch.
VC Branch Name/Key	Key for the branch, which is unique to each branch.
Bid(Subnet Name)	<p>Branch ID (BID) of the subnet.</p> <p>In the example above, the managed device displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs.</p> <p>Branches that are in UP state and do not have a Bid(Subnet Name) means that the IAP is connected to a managed device which did not assign any bid for any subnet. In the above example, "Paris-CB:D3:16" branch is UP and does not have a Bid(Subnet Name) information. This means that either the IAP is connected to a backup managed device or connected to a primary managed device without any distributed L2 or L3 subnets.</p> <p>For more information on bid-per-subnet-per-branch and distributed L2 and L3 subnets, see the <i>DHCP Configuration</i> chapter of the Aruba <i>Instant Access Point 6.2.1.0-3.3 User Guide</i>.</p>
Tunnel End Points	Displays tunnel end points for the branch.

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following modifications were introduced: <ul style="list-style-type: none">▪ The output parameter, <code>Name</code> is modified as <code>VC Name</code>.▪ The output parameter, <code>Key</code> is modified as <code>VC Branch Name</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show iap trusted-branch-db

```
show iap trusted-branch-db
```

Description

Displays the details of IAP trusted branch database information.

Examples

The following example shows the details of IAP trusted branch database information:

```
(host) [mynode] (config) #show iap trusted-branch-db

Trusted Branch Validation: Enabled
IAP Trusted Branch Table
-----
Branch MAC
-----
01:01:0e:3e:4c:33
```

The following example shows details of IAP trusted branch database information:

```
(host) #show iap trusted-branch-db

Trusted Branch Validation: Disabled
IAP Trusted Branch Table
-----
Branch MAC
-----
(allow all as trusted branch)
```

The output of this command includes the following parameters:

Parameter	Description
Branch MAC	MAC address of the trusted IAP branch.

Related Commands

Command	Description
hostname	This command changes the hostname of the Mobility Conductor, standby controller, or managed device.

Command	Description
iap trusted-branch-db	This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Enable or Configuration mode on managed devices.

show ids

```
show ids
  ap-classification-rule
  ap-rule-matching
  dos-profile
  general-profile
  impersonation-profile
  management-profile
  profile
  rap-wml-server-profile
  rap-wml-table-profile
  rate-thresholds-profile
  signature-matching-profile
  signature-profile
  unauthorized-device-profile
  wms-general-profile
  wms-local-system-profile
```

Description

This command displays the list of all IDS profiles. Click the parameter links below to view the corresponding show commands.

Parameter	Description
ap-classification-rule	Displays the IDS AP Classification Rule Profile.
ap-rule-matching	Displays the IDS Active AP Rules Profile.
dos-profile	Displays an IDS DoS Profile.
general-profile	Displays an IDS General Profile.
impersonation-profile	Displays an IDS Impersonation Profile.
management-profile	Displays the management event correlation for IDS event traps and sylogs (logs).
profile	Displays all ids profiles or displays a specific profile name.
rap-wml-server-profile	Displays an IDS Rate Thresholds Profile.
rap-wml-table-profile	Displays an IDS Rate Thresholds Profile.
rate-thresholds-profile	Displays an IDS Rate Thresholds Profile.
signature-matching-profile	Displays an IDS Signature Matching Profile.
signature-profile	Displays an IDS Signature Profile.

Parameter	Description
unauthorized-device-profile	Displays an IDS Unauthorized Device Profile.
wms-general-profile	Displays general statistics for the WMS configuration.
wms-local-system-profile	Displays statistics for the WMS Local System Profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ids ap-classification-rule

id-classification-rule <rule-name>

Description

Displays the IDS AP Classification Rule Profile. Issue this command without the <rule-name> option to view the AP Classification Rule Profile list. Add the rule name option to display values for the rule.

Parameter	Description
<rule-name>	Enter the AP classification rule profile name.

Example

The following example is the show command *without* the rule name option:

```
(host) [mynode] (config) #show ids ap-classification-rule
IDS AP Classification Rule Profile List
-----
Name                References  Profile Status
----                -
exclude-ssid-rule   1
rule1                1
rule2                1
Total:3
```

In the example above, the **Reference** column indicates the number of references to the rule named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

Optionally, you can enter a rule name to view the parameters for that rule. For example:

```
(host) [mynode] (config) #show ids ap-classification-rule rule1
IDS AP Classification Rule Profile "rule1"
-----
Parameter                Value
-----
SSID                      Aruba-ap
Match SSIDs               true
Min SNR value             0
Max SNR value             255
Discovered APs count      2
Check for Min Discovered APs true
Classify To AP Type       suspected-rogue
Confidence level increase 5
```

Related Commands

Command	Description
ids ap-classification-rule	This command configures the IDS AP classification rule profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids ap-rule-matching

Description

Displays the IDS Active AP Rules Profile. Issue this command to view the Active AP Rules Profile list.

Example

The following command displays AP Rule names information:

```
(host) [mynode] (config) #show ids ap-rule-matching

IDS Active AP Rules Profile
-----
Parameter      Value
-----
AP Rule name   snr0
AP Rule name   rule1
AP Rule name   rule2
AP Rule name   exclude-ssid-rule
```

In the above example, the rule names in the *Value* column have been activated by the **ids ap-rule-matching** command.

Related Commands

Command	Description
ids ap-rule-matching	This command configures the IDS active AP rules profile by enabling an AP classification rule.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config or Enable mode on Mobility Conductor.

show ids dos-profile

```
show ids dos-profile <profile-name>
```

Description

Shows an IDS DoS Profile. Issue this command without the <profile-name> parameter to display an IDS DoS Profile.

Parameter	Description
<profile-name>	Name of an IDS DoS Profile.

Examples

The following example shows that the controller has four configured DoS Profiles:

```
(host) [mynode] (config) #show ids dos-profile

IDS Denial Of Service Profile List
-----
Name      References Profile Status
-----
default   4
test      0
test1     1
Wizard-test 1
Wizard-test2 1

Total: 5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays a partial output for the profile **test1**:

```
(host) [mynode] (config) #show ids dos-profile test1
Parameter                                     Value
-----
Detect Disconnect Station Attack              true
Disconnect STA Assoc Response Theshold       5
Disconnect STA Deauth and Disassoc Theshold  8
Disconnect STA Detection Quiet Time          900 sec
Detect AP Flood Attack                        false
AP Flood Threshold                           50
AP Flood Increase Time                       3 sec
AP Flood Detection Quiet Time                900 sec
Detect Client Flood Attack                   false
```

```

Client Flood Threshold 150
Client Flood Increase Time 3 sec
Client Flood Detection Quiet Time 900 sec
Detect EAP Rate Anomaly false
EAP Rate Threshold 60
EAP Rate Time Interval 3 sec
EAP Rate Quiet Time 900 sec
Detect CTS Rate Anomaly false
CTS Rate Threshold 5000
CTS Rate Time Interval 5 sec
CTS Rate Quiet Time 900 sec
Detect RTS Rate Anomaly false
RTS Rate Threshold 5000
RTS Rate Time Interval 5 sec
RTS Rate Quiet Time 900 sec
Detect GHOST TUNNEL SERVER Attack false
Detect GHOST TUNNEL CLIENT Attack false
GHOST TUNNEL Attack Beacon Detection Threshold 200
GHOST TUNNEL Attack Probe Request Detection Threshold 10
GHOST TUNNEL Attack Detection Time Interval 60 sec
GHOST TUNNEL Attack Detection Time Interval 60 sec
Ghosttunnel Attack Detection SERVER Quiet Time 900 sec
Ghosttunnel Attack Detection CLIENT Quiet Time 900 sec
Detect Rate Anomalies false
Rate Thresholds for Assoc Frames default
Rate Thresholds for Disassoc Frames default
Rate Thresholds for Deauth Frames default
...

```

For a detailed explanation of the output shown above, see the [ids dos-profile](#) command.

Related Commands

Command	Description
ids dos-profile	This command configures IDS DoS Profiles.

Command History

Release	Modification
ArubaOS 8.10.0.0	<p>The following parameters were added:</p> <ul style="list-style-type: none"> ■ Detect GHOST TUNNEL SERVER Attack ■ Detect GHOST TUNNEL CLIENT Attack ■ GHOST TUNNEL Attack Beacon Detection Threshold ■ GHOST TUNNEL Attack Probe Request Detection

Release	Modification
	Threshold <ul style="list-style-type: none"> ■ GHOST TUNNEL Attack Detection Time Interval ■ GHOST TUNNEL Attack Detection Time Interval ■ Ghosttunnel Attack Detection SERVER Quiet Time ■ Ghosttunnel Attack Detection CLIENT Quiet Time
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids general-profile

```
show ids general-profile <profile-name>
```

Description

Displays an IDS General Profile. Issue this command without the <profile-name> parameter to display the IDS General Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS General Profile.

Examples

The following example shows that the managed device has four configured General Profiles:

```
(host) [mynode] (config) # show ids general-profile
IDS General Profile List
-----
Name           References  Profile Status
----           -
default        2
helen          0
wired-lb       1
Wizard-test2  1
Total: 4
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the settings for the profile **default**:

```
(host) [mynode] (config) #show ids general-profile default
IDS General Profile "default"
-----
Parameter                               Value
-----
Adhoc AP Max Unseen Timeout              180 sec
Adhoc (IBSS) AP Inactivity Timeout       5 sec
AP Inactivity Timeout                    20 sec
AP Max Unseen Timeout                    600 sec
AP Neighbors Message Interval            180 sec
AP Neighbors Message                     false
Client Detection Mode                    normal
Frame Types for RSSI calculation         ba pr dlow dnull mgmt ctrl
```

```

IDS Event Generation on AP          logs-and-traps
Max Monitored Devices              0
Max Monitored APs                  0
Max Unassociated Stations           512
Min Potential AP Beacon Rate       25 %
Min Potential AP Monitor Time      2 sec
Mobility Manager RTLS              false
Monitored Device Stats Update Interval 0 sec
Packet SNR Threshold               0
Send Adhoc Info to Controller      false
Signature Quiet Time                900 sec
STA Inactivity Timeout              60 sec
STA Max Unseen Timeout              600 sec
Station RSSI Message Interval      60 sec
Station RSSI Message               false
Radio Info Ext Message Interval    300 sec
Stats Update Interval              60 sec
Unclassified AP Update             false
Unclassified STA Update            false
Unclassified Device Update Interval 60 sec
Wired Containment                  false
Wired Containment of AP's Adj MACs false
Wired Containment of Suspected L3 Rogue false
Wireless Containment               deauth-only
Wireless Containment Deauth Reason 3
Debug Wireless Containment         false
WMS Client Monitoring              all

```

The output of this command includes the following parameters:

Parameter	Description
Adhoc AP Max Unseen Timeout	Ageout time in seconds since ad hoc (IBSS) AP was last seen.
Adhoc (IBSS) AP Inactivity Timeout	Ad hoc (IBSS) AP inactivity timeout in number of scans.
AP Inactivity Timeout	Time, in seconds, after which an AP is aged out.
AP Max Unseen Timeout	Ageout time, in seconds, since AP was last seen.
Frame Types for RSSI calculation	Frame types used in AM RSSI calculation.

Parameter	Description
IDS Event Generation on AP	Enable or disable IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch.
Max Monitored Devices	Maximum number of APs and stations that can be monitored. This number does not include stations that are not associated to any AP. Within this max value, the AP reserves a buffer for stations that are associated locally.
Max Monitored APs	Maximum number of monitored APs. Default value: 0
Max Monitored Stations	Maximum number of monitored stations.
Max Unassociated Stations	Maximum number of unassociated stations.
Min Potential AP Beacon Rate	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.
Min Potential AP Monitor Time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.
Mobility Manager RTLS	Shows if RTLS communication with the configured mobility-manager is enabled or disabled.
Monitored Device Stats Update Interval	Time interval, in seconds, for AP to update the switch with stats for monitored devices. Minimum is 60.
Packet SNR Threshold	The packet Signal to Noise Ratio (SNR) threshold. All packets with SNR below this threshold is dropped from IDS and ARM processing. No packets are dropped if the threshold is set to 0.
Send Adhoc Info to Controller	Enable or disable sending adhoc information to the managed device from the AP.
Signature Quiet Time	After a signature match is detected, the time to wait, in seconds, to resume checking.
STA Inactivity Timeout	Time, in seconds, after which a station is aged out.
STA Max Unseen Timeout	Time, in seconds, after which an AP is aged out.

Parameter	Description
Station RSSI Message Interval	Interval, in seconds, at which the AP delivers station RSSI messages to the management server. The range value is 1-36000. The default value is 1 second.
Station RSSI Message	Enables or disables station RSSI messages. The default value is disabled.
Stats Update Interval	Interval, in seconds, for the AP to update the managed device with statistics. This setting takes effect only if the Aruba Mobility Manager is configured. Otherwise, statistics update to the managed device is disabled.
Unclassified AP Update	Enables or disables classification updates for monitored APs. If this option is enabled, there is a decrease in the delay with which the devices are classified. The default value is disabled.
Unclassified STA Update	Enables or disables classification updates for monitored clients. If this option is enabled, there is a decrease in the delay with which the devices are classified. The default value is disabled.
Unclassified Device Update Interval	The time interval, in seconds, for the AP to send the WMS a list of unclassified APs and clients. The range value is 30-36000 seconds. The default value is 60 seconds.
Wired Containment	Shows if the profile has enabled or disabled containment from the wired side.
Wired Containment of AP's Adj MACs	Shows if the profile has enabled or disabled wired containment of MACs offset by one from APs BSSID.
Wired Containment of Suspected L3 Rogue	Shows if the profile has enabled or disabled the feature to identify and contain an AP with a preset wired MAC address that is completely different from the AP's BSSID. where the MAC address that the AP provides to wireless clients as a 'gateway MAC' is offset by one character from its wired MAC address.
Wireless Containment	Shows if the profile has enabled or disabled containment from the wireless side.
Wireless Containment Deauth Reason	Specify deauth reason for containment from the wireless side. Range: 1 - 134 Default: 3

Parameter	Description
Debug Wireless Containment	Shows if the profile has enabled or disable debugging of containment from the wireless side.
Wired Containment of AP's Adj MACs	Enable or disable wired containment of MACs offset by one from APs BSSID.

Related Commands

Command	Description
ids general-profile	This command configures an IDS general profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	The output of the command was modified to display Wireless Containment Deauth Reason and Max Monitored APs .
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids impersonation-profile

```
show ids impersonation-profile <profile-name>
```

Description

Displays an IDS Impersonation Profile. Issue this command without the <profile-name> parameter to display the IDS Impersonation Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Impersonation Profile.

Examples

The following example displays that the Mobility Conductor has five configured Impersonation Profiles:

```
(host) [mynode] (config) #show ids impersonation-profile

IDS Impersonation Profile List
-----
Name           References  Profile Status
----           -
default        4
test           0
test1          1
Wizard-test    1
Wizard-test2   1

Total: 5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the configuration settings for the profile **test1**:

```
(host) (config) #show ids impersonation-profile test1

IDS Impersonation Profile "test1"
-----
Parameter                               Value
-----
Detect AP Impersonation                   false
Protect from AP Impersonation             false
Beacon Diff Threshold                     50 %
Beacon Increase Wait Time                 3 sec
```

```

Detect AP Spoofing           true
Detect Beacon Wrong Channel  false
Beacon Wrong Channel Detection Quiet Time 900 sec
Detect Hotspotter Attack     true
Hotspotter Quiet Time       900 sec

```

The output of this command includes the following parameters:

Parameter	Description
Detect AP Impersonation	Shows of the profile has enabled or disabled detection of AP impersonation.
Protect from AP Impersonation	Shows if AP impersonation is enabled or disabled for the profile. When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a DoS attack.
Beacon Diff Threshold	Percentage increase in beacon rates that triggers an AP impersonation event.
Beacon Increase Wait Time	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.
Detect AP Spoofing	AP Spoofing detection is enabled
Detect Beacon Wrong Channel	Disable detection of beacons advertising the incorrect channel
Beacon Wrong Channel Detection Quiet Time	Wait 90 seconds after detecting a beacon with the wrong channel after which the check can be resumed.
Detect Hotspotter Attack	Enable detection of the Hotspotter attack to lure away valid clients.
Hotspotter Quiet Time	Wait 90 seconds after detecting an attempt to Use the Hotspotter tool against clients.

Related Commands

Command	Description
ids impersonation-profile	This command configure IDS impersonation profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids management-profile

Description

Displays the management event correlation for IDS event traps and sylogs (logs).

Example

The following example displays the current management status:

```
(host) [mynode] (config) #show ids management-profile

IDS Management Profile
-----
Parameter          Value
-----          -
IDS Event Correlation    logs-and-traps
Event Correlation Quiet Time 900 sec
```

The display output of the above command includes:

Parameter	Description
IDS Event Correlation	Management profile is set for logs-and-traps.
Event Correlation Quiet Time	The time to wait, 900 seconds, before the event can be raised again.

Related Commands

Command	Description
ids management-profile	This command configures the IDS WMS management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids profile

```
show ids profile <profile-name>
```

Description

Displays all ids profiles or displays a specific profile name. Issue this command without the <profile-name> parameter to display the list of IDS Profiles. Include a profile name to display detailed information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Profile.

Examples

The following example shows that the controller has seven configured IDS Profiles:

```
(host) [mynode] (config) #show ids profile

IDS Profile List
-----
Name           References  Profile Status
-----
default        5
test           0
test-tarpit    1
test-wired-lb  0
test1          0
Wizard-test    0
Wizard-test2  0

Total: 7
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the configuration settings for the profile **test1**:

```
(host) [mynode] (config) #show ids profile test1

IDS Profile "test1"
-----
Parameter                               Value
-----
IDS General profile                       test1
IDS Signature Matching profile            test1
IDS DOS profile                           test1
```

```
IDS Impersonation profile      test1
IDS Unauthorized Device profile test1
```

The output of this command includes the following parameters:

Parameter	Description
IDS General profile	Name of a IDS General profile to be applied to an AP or AP group.
IDS Signature Matching profile	Name of a IDS Signature Matching profile to be applied to an AP or AP group.
IDS DOS profile	Name of a IDS DoS profile to be applied to an AP or AP group.
IDS Impersonation profile	Name of a IDS Impersonation profile to be applied to an AP or AP group.
IDS Unauthorized Device profile	Name of a IDS Unauthorized Device profile to be applied to an AP or AP group.

Related Commands

Command	Description
ids profile	This command configures the IDS profile .

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids rap wml server profile

```
show ids rap-wml-server-profile <server-name>
```

Description

Shows a IDS Remote AP WML server profile. Issue this command without the `<profile-name>` parameter to display the IDS Rate Threshold Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><server-name></code>	Name of an IDS Remote AP WML server profile.

Related Commands

Command	Description
ids rate-thresholds-profile	This command configures the IDS Rate Threshold profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids rap wml table profile

```
show ids rap-wml-table-profile <table-name>
```

Description

Shows an IDS RAP WML Table Profile.

Parameter	Description
<table-name>	Name of an IDS RAP WML Table Profile.

Related Commands

Command	Description
ids rap-wml-table-profile	This command configures an IDS remote AP WML table profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids rate-thresholds-profile

```
show ids rate-thresholds-profile <profile-name>
```

Description

Shows an IDS Rate Thresholds Profile. Issue this command without the <profile-name> parameter to display the IDS Rate Threshold Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Rate Threshold Profile.

Examples

The following example shows that the controller has three configured IDS Rate Threshold profiles:

```
(host) [mynode] (config) #show ids rate-thresholds-profile

IDS Rate Thresholds Profile List
-----
Name                               References  Profile Status
----                               -
default                             20
probe-request-response-thresholds  10          Predefined
test                                 0

Total: 3
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the configuration settings for the profile **test**:

```
(host) [mynode] (config) #show ids rate-thresholds-profile test

IDS Rate Thresholds Profile "test"
-----
Parameter                          Value
-----
Channel Increase Time               15 sec
Channel Quiet Time                  900 sec
Channel Threshold                    300
Node Time Interval                   15 sec
Node Quiet Time                      900 sec
Node Threshold                       200
```


The output of this command includes the following parameters:

Parameter	Description
Channel Increase Time	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
Channel Quiet Time	The time that must elapse after a channel rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.
Channel Threshold	Number of a specific type of frames that must be exceeded within a specific interval in an entire channel to trigger an alarm.
Node Time Interval	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
Node Quiet Time	The time that must elapse after a node rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.
Node Threshold	Number of a specific type of frames that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.

Related Commands

Command	Description
ids rate-thresholds-profile	This command configures the IDS Rate Threshold profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids signature-matching-profile

```
show ids signature-matching-profile <profile-name>
```

Description

Shows an IDS Signature Matching Profile. Issue this command without the <profile-name> parameter to display the entire IDS Signature Matching Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Signature Matching Profile.

Examples

The following example shows that the Mobility Conductor has four configured Signature Matching Profiles:

```
(host) [mynode] (config) #show ids signature-matching-profile

IDS Signature Matching Profile List
-----
Name           References  Profile Status
-----
default        4
test1          1
Wizard-test    1
Wizard-test2   1

Total: 4
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the configuration settings for the profile **test1**:

```
(host) [mynode] (config) #show ids signature-matching-profile test1

IDS Signature Matching Profile "test1"
-----
Parameter      Value
-----
IDS Signature   Deauth-Broadcast
IDS Signature   Disassoc-Broadcast
```

The output of this command includes the following parameters:

Parameter	Value
IDS Signature	Broadcast is not authorized.
IDS Signature	Disassociate broadcast.

Related Commands

Command	Description
ids management-profile	This command configures an IDS signature matching profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids signature-profile

```
show ids signature-profile <profile-name>
```

Description

Shows an IDS Signature Profile. Issue this command without the <profile> parameter to display the entire IDS Signature Profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Signature Profile.

Examples

The following example shows that the controller has eight configured Signature Profiles:

```
(host) [mynode] (config) #show ids signature-profile

IDS Signature Profile List
-----
Name                References  Profile Status
----                -
AirJack             1          Predefined
ASLEAP              1          Predefined
Deauth-Broadcast   1          Predefined
default             1
Netstumbler Generic 1          Predefined
Netstumbler Version 3.3.0x 1          Predefined
Null-Probe-Response 1          Predefined
sample              0

Total: 8
```

The following example displays the configuration settings for the profile **AirJack**:

```
(host) [mynode] (config) # show ids signature-profile
IDS Signature Profile "AirJack" (predefined)
-----
Parameter  Value
-----
Frame Type  beacon SSID = AirJack
```

The output of this command includes the following parameters:

Parameter	Description
Frame Type	Type of 802.11 frame. For each type of frame, further parameters may be included to filter and detect only the required frames. <ul style="list-style-type: none"> ▪ assoc: Association frame type. ▪ auth: Authentication frame type. ▪ beacon: Beacon frame type. ▪ control: All control frames. ▪ data: All data frames. ▪ deauth: Deauthentication frame type. ▪ disassoc: Disassociation frame type. ▪ mgmt: Management frame type. ▪ probe-request: Probe request frame type. ▪ probe-response: Probe response frame type. ▪ ssid: For beacon, probe-request, and probe-response frame types, the SSID as either a string or hex pattern. ▪ ssid-length: For beacon, probe-request, and probe-response frame types, the length, in bytes, of the SSID.
payload	Pattern at a fixed offset in the payload of an 802.11 frame.
sequence number	Sequence number of the frame.
src- mac	Source MAC address in the 802.11 frame header.
dst- mac	Source MAC address in the 802.11 frame header.
bssid	BSSID field in the 802.11 frame header.

Related Commands

Command	Description
ids signature-profile	This command configures the signature profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config mode on Mobility Conductor.

show ids unauthorized-device-profile

```
show ids unauthorized-device-profile <profile-name>
```

Description

Show an IDS Unauthorized Device Profile. Issue this command without the <profile-name> parameter to display the IDS Unauthorized Device Profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an IDS Unauthorized Device Profile.

Examples

The following example shows that the Mobility Conductor has five configured Unauthorized Device Profiles:

```
(host) [mynode] (config) #show ids unauthorized-device-profile

IDS Unauthorized Device Profile List
-----
Name           References  Profile Status
-----
default        4
test           0
test1          1
Wizard-test    1
Wizard-test2   1

Total: 5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The following example displays the configuration settings for the profile **test1**:

```
(host) [mynode] (config) #show ids unauthorized-device-profile test1

IDS Unauthorized Device Profile "test1"
IDS Unauthorized Device Profile "default"
-----
Parameter                                           Value
-----
Protect 802.11n High Throughput Devices             false
Protect 40MHz 802.11n High Throughput Devices       false
Detect Active 802.11n Greenfield Mode                false
```

```

Detect Adhoc Networks false
Protect from Adhoc Networks false
Protect from Adhoc Networks - Enhanced false
Detect Adhoc Network Using Valid SSID true
Adhoc Network Using Valid SSID Quiet Time 900 sec
Allow Well Known MAC N/A
Detect Devices with an Invalid MAC OUI false
MAC OUI detection Quiet Time 900 sec
Detect Misconfigured AP false
Protect Misconfigured AP false
Detect Bad WEP false
Privacy false
Require WPA false
Valid 802.11g channel for policy enforcement N/A
Valid 802.11a channel for policy enforcement N/A
Valid and Protected SSIDs N/A
Valid MAC OUIs N/A
Rogue AP Classification true
Overlay Rogue AP Classification true
OUI-based Rogue AP Classification true
Propagated Wired MAC based Rogue AP Classification true
Rogue Containment false
Suspected Rogue Containment false
Suspected Rogue Containment Confidence Level 60
Detect Station Association To Rogue AP true
Detect Unencrypted Valid Clients true
Unencrypted Valid Client Detection Quiet Time 900 sec
Detect Valid Client Misassociation true
Detect Valid SSID Misuse false
Protect SSID false
Protect Valid Stations false
Valid Wired MACs N/A
Vendor Specific OUI /OUI-Type for containment exclusion N/A

Detect Windows Bridge true
Protect Windows Bridge false
Detect Wireless Bridge false
Wireless Bridge detection Quiet Time 900 sec
Detect Wireless Hosted Network true
Wireless Hosted Network Quiet Time 900 sec
Protect From Wireless Hosted Networks false

```

The output of this command includes the following parameters:

Parameter	Description
Protect 802.11n High Throughput Devices	Shows if the profile enables or disables protection of HT (802.11n) devices.

Parameter	Description
Protect 40MHz 802.11n High Throughput Devices	Shows if the profile enables or disables protection of HT (802.11n) devices operating in 40 MHz mode.
Detect Active 802.11n Greenfield Mode	Shows if the profile enables or disables detection of HT devices advertising greenfield preamble capability.
Detect AdHoc Networks	Shows if the profile has enabled or disabled detection of ad hoc networks.
Protect from Adhoc Networks	Shows if the profile has enabled or disabled protection from WPA or WPA2 ad hoc networks.
Protect from Adhoc Networks-Enhanced	Shows if the profile has enabled or disabled protection from WEP or Open ad hoc networks.
Detect Valid SSID Misuse	Shows if the detect valid SSID misuse is enabled (true) or disabled (false).
Adhoc Network Using Valid SSID Quiet Time	Shows time to wait, in seconds, after detecting an ad hoc network using a valid SSID, after which the check can be resumed.
Allow Well Known MAC	Shows if the profile allows devices with known MAC addresses to classify rogue APs.
Detect Devices with an Invalid MAC OUI	Shows if the profile has enabled or disabled checking of the first three bytes of a MAC address, known as the OUI, assigned by the IEEE to known manufacturers.
MAC OUI detection Quiet Time	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.

Parameter	Description
Detect Misconfigured AP	Shows if the profile has enabled or disabled detection of misconfigured APs.
Protect Misconfigured AP	Shows if the profile has enabled or disabled protection of misconfigured APs.
Detect Bad WEP	Shows if the profile has enabled or disabled detection of WEP initialization vectors that are known to be weak or repeating.
Privacy	Shows if the profile has enabled or disabled encryption as a valid AP configuration.
Require WPA	Shows if the Mobility Conductor will flag any valid AP not using WPA as a misconfigured AP.
Valid 802.11g channel for policy enforcement	A list of valid 802.1b or 802.1g channels that third-party APs are allowed to use.
Valid 802.11a channel for policy enforcement	A list of valid 802.11a channels that third-party APs are allowed to use.
Valid and Protected SSIDs	A list of valid and protected SSIDs.
Valid MAC OUIs	A list of valid MAC OUIs.
Rogue AP Classification	Shows if the profile has enabled or disabled rogue AP classification.
Overlay Rogue AP Classification	Shows if the Mobility Conductor allows APs that are plugged into the wired side of the network to be classified as "suspected rogue" instead of "rogue".

Parameter	Description
OUI-based Rogue AP Classification	Shows if OUI-based rogue AP classification is enabled or disabled.
Propagated Wired MAC based Rogue AP Classification	Shows if rogue AP classification through propagated wired MACs is enabled or disabled.
Rogue Containment	Shows if the Mobility Conductor will automatically shut down rogue APs.
Suspected Rogue Containment	Shows if the Mobility Conductor will automatically treat suspected rogue APs as interfering APs.
Suspected Rogue Containment Confidence Level	Confidence level of suspected Rogue AP to trigger containment, expressed as a percentage.
Detect Station Association To Rogue AP	Shows if the profile has been configured to detect station association to a rogue AP.
Detect Unencrypted Valid Clients	Shows if the profile has enabled or disabled detection of unencrypted valid clients.
Unencrypted Valid Client Detection Quiet Time	Shows the time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.
Detect Valid Client Misassociation	Shows if the profile has enabled or disabled detection of a misassociation between a valid client and an unsafe AP.
Detect Valid SSID Misuse	Shows if the profile has enabled or disabled detection of Interfering or Neighbor APs using valid or protected SSIDs.
Protect SSID	Shows if the profile has enabled or disabled use of SSID by valid APs only.

Parameter	Description
Protect Valid Stations	Shows if the Mobility Conductor will allow valid stations to connect to a non-valid AP.
Valid Wired MACs	List of valid and protected SSIDs.
Vendor Specific OUI/OUI-Type for containment exclusion	Shows the details of vendor specific IE information for containment exclusion.
Detect Windows Bridge	Shows if the profile has enabled or disabled detection of Windows station bridging.
Protect Windows Bridge	Shows if the profile has enabled or disabled protection of Windows station bridging.
Detect Wireless Bridge	Shows if the profile has enabled or disabled detection of wireless bridging.
Wireless Bridge detection Quiet Time	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.
Protect From Wireless Hosted Networks	Shows if the profile has enabled or disabled detection of a wireless hosted network.
Wireless Hosted Network Quiet Time	The wireless hosted network detection feature sends a log message and trap when a wireless hosted network is detected. The quiet time displayed in this field displays the amount of time, in seconds, that must elapse after a wireless hosted network log message or trap has been triggered before an identical log message or trap can be sent again.

Parameter	Description
Protect From Wireless Hosted Networks	Shows if the profile has enabled or disabled containment on a wireless hosted network by launching a DoS attack to disrupt associations between a Windows 7 software-enabled Access Point (softAP) and a client, and disrupt associations between the client that is hosting the softAP and any access point to which the host connects.

Related Commands

Command	Description
ids unauthorized-device-profile	This command configure the Unauthorized Device profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameter, Vendor Specific OUI / OUI-Type for containment exclusion was introduced.
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license.	Config mode on Mobility Conductor.

show ids wms-general-profile

```
show ids wms-general-profile
```

Description

Displays general statistics for the wms configuration.

Example

The following example shows per-channel statistics for all monitored APs:

```
(host) [mynode] (config) #show ids wms-general-profile

IDS WMS General Profile
-----
Parameter                               Value
-----
AP poll interval                         60000 msec
AP poll retries                           3
AP ageout interval                       0 minutes
Adhoc AP ageout interval                 31 minutes
Station ageout interval                 100 minutes
Statistics update                         true
Persistent Neighbor APs                  true
Persistent Valid STAs                    false
AP learning                              false
Propagate Wired Macs                     true
Collect Stats for Monitored APs and Clients false
Learn System Wired Macs                   false
```

The output of this command includes the following information:

Column	Description
AP poll interval	Interval, in milliseconds, for communication between the controller and AMs. The controller contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.
AP poll retries	Maximum number of failed polling attempts before the polled AM is considered to be down.
AP ageout interval	Time, in minutes, that an AP must remain unseen by any probes before it is deleted from the database.

Column	Description
Adhoc AP ageout interval	Time, in minutes, that an ad hoc (IBSS) AP remains unseen before it is deleted (ageout) from the database.
Station ageout interval	Time, in minutes, that a client must remain unseen by any probes before it is deleted from the database.
Statistics update	Shows the status of the statistics updates in the database.
Persistent Neighbor APs	Shows the status of known AP neighbors.
Persistent Valid STAs	Shows the status of known AP neighbors.
AP learning	Shows the status of "learning" of non-Aruba APs.
Propagate Wired Macs	Shows if the controller has enabled or disabled the propagation of the gateway wired MACs.
Collect Stats for Monitored APs and Clients	Shows if the master/ conductor controller will collect up to 25,000 statistic entries for monitored APs and clients.
Learn System Wired Macs	Shows the status of "learning" of wired MACs at the controller.

Related Commands

Command	Description
ids wms-general-profile	This command configures the IDS WLAN management system (WMS) general profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ids wms-local-system-profile

```
ids wms-local-system-profile
max-ap-threshold <max-ap-threshold>
```

Description

Displays statistics for the WMS Local System Profile settings. The configuration parameters in IDS WMS Local System Profile enables local termination of the WMS service, sets maximum thresholds for the maximum number of managed APs and stations, and defines the intervals at which valid AP, rogue AP, and station data is sent to the managed device. Issue this command to view the local WMS service profile settings .

Example

The following commands first set the interval time for repopulating the MAC table to 10 minutes and then sets the maximum number of APs to 100:

```
(host)[mynode] (config) #show ids wms-local-system-profile
IDS WMS Local System Profile
-----
Parameter                               Value      Set
-----
Max AP Threshold                         100
Max STA Threshold                        0
Max RBTtree Entries                      3
Max System Wired MACs                    1000
Override Service Termination            false
Periodic AP Snapshot Interval           180 minutes
Periodic Rogue AP Snapshot Interval     30 minutes
Periodic STA Snapshot Interval          180 minutes
System Wired MAC Update Interval         8
```

The output of this command includes the following information:

Table 12: *IDS WMS Local System Profile Settings*

Parameter	Description
Max AP Threshold	The max threshold for the total number of APs.
Max STA Threshold	The max threshold for the total number of stations.
Max RBTtree Entries	The max threshold for the total number of AP and station RBTtree entries.
Max System Wired MACs	The max number of system wired MAC table entries learned by the managed device.

Parameter	Description
Override Service Termination	If enabled, this feature overrides the system-determined termination mode, and terminates WMS service at the managed device to which the AP is associated.
Periodic AP Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored APs. The (AMON) messages comprising the snapshot will be spread over this interval.
Periodic Rogue AP Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored Rogue APs. The (AMON) messages comprising the snapshot will be spread over this interval.
Periodic STA Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored clients. The (AMON) messages comprising the snapshot will be spread over this interval.
System Wired MAC Update Interval	The interval, in minutes, for repopulating the system wired MAC table at the managed device.

Related Commands

Release	Modification
mgmt-server	Configures the management server profile.
ids management-profile	Manage the events correlation for IDS event traps and syslogs (logs).
ids wms-local-system-profile	This command configures the WMS service to terminate on individual managed devices instead of Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show ifmap

Syntax

```
show ifmap
  cppm
  state cppm
  statistics cppm
```

Descriptions

Issue this command to show the ClearPass Policy Manager IF-MAP configuration profile and the IP-MAP connection state.

Parameter	Description
cppm	Shows the ClearPass Policy Manager IF-MAP profile parameters and their values.
state cppm	Shows the ClearPass Policy Manager IF-MAP connection state including if it is enabled, and the servers and their state.
statistics cppm	Shows the statistics data.

Example

To configure this feature using the CLI:

```
(host) [mynode] (config) #ifmap
(host) [mynode] (config) #ifmap cppm
(host) [mynode] (CPPM IF-MAP Profile) #server host <host>
(host) [mynode] (CPPM IF-MAP Profile) #port <port>
(host) [mynode] (CPPM IF-MAP Profile) #passwd <psswd>
(host) [mynode] (CPPM IF-MAP Profile) #enable
```

This show command show if the CCPM interface is enable and the ClearPass Policy Manager server IP address, username and password.

```
(host)[mynode] (CPPM IF-MAP Profile) #show ifmap cppm
CPPM IF-MAP Profile
-----
Parameter                Value
-----
CPPM IF-MAP Interface    Enabled
CPPM IF-MAP Server       10.10.10.10:443 admin/*****
```

This show command shows if state of all enabled ClearPass Policy Manager servers.

```
(host)[mynode] (CPPM IF-MAP Profile) #show ifmap state cppm
CPPM IF-MAP Connection State [Interface: Enabled]
-----
Server                State
-----
10.4.191.32:443      UP
```

Related Commands

Command	Description
ifmap	This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass so that it can make more accurate decisions about what types of devices are connecting to the network

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode

show image version

Syntax

```
show image version  
type
```

Description

Display the current system image version on both partition 0 and 1.

Parameter	Description
type	Displays the System image type.

Example

The following example shows that the managed device is running ArubaOS 8.0 and booting off partition 0:1.

```
(host)[mynode] #show image version  
-----  
Partition           : 0:0 (/mnt/disk1)  
Software Version    : ArubaOS 8.0.0.0-svcs-ctrl (Digitally Signed -  
Developer/Internal Build)  
Build number        : 0000  
Label               : ssetty@ss_sc_new-ENG.0000  
Built on            : Wed Jun 8 14:46:22 IST 2016  
-----  
Partition           : 0:1 (/mnt/disk2) **Default boot**  
Software Version    : ArubaOS 8.0.0.0-svcs-ctrl (Digitally Signed -  
Developer/Internal Build)  
Build number        : 0000  
Label               : ssetty@ss_sc_new-ENG.0000  
Built on            : Thu Jun 16 12:53:57 IST 2016
```

The output of this command includes the following parameters:

Parameter	Description
Partition	Partition number and name. The default boot partition will display a **Default boot** notice by the partition name.
Software Version	Version of ArubaOS software running on the partition.

Parameter	Description
Build number	Build number for the software version.
Label	The label parameter can display additional information for the build. By default, this value is the software build number.
Built on	Date the software build was created.

Following is an example of `show image version type` command:

```
(host) [mynode] #show image version type
This image is development build
```

Related Commands

Command	Description
show ap image-preload status	This command displays the list of APs that will preload a new version of software from a controller with the AP preload feature activated.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show interface

```
show interface
  cellular
  counters
  gigabitethernet
  list
  loopback
  mgmt
  port-channel
  tunnel
  vlan
```

Description

This command displays the list of all interfaces. Click the parameter links below to view the corresponding show commands.

Parameter	Description
cellular	Displays the access groups configured on the cellular interface.
counters	Displays a table of L2 interfaces counters.
gigabitethernet	Displays information about a specified Gigabit Ethernet port.
list	Displays interfaces for all platforms supported by current SC version.
loopback	Displays information about the Loopback IP interface.
mgmt	Displays information about management Ethernet IP interfaces.
port-channel	Displays information about a specified port-channel interface.
tunnel	Displays information about tunnel interfaces.
vlan	Displays information about a specified VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show interface cellular access-group

show interface cellular access-group

Description

Lists the access groups configured on the cellular interface.

Example

```
(host) [mynode] #show interface cellular access-group
Cell Interface:
session access list 3 is configured
```

Related Commands

Command	Description
interface cellular	This command allows you to specify an ingress or egress ACL to the cellular interface of an EVDO modem.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show interface counters

show interface counters

Description

Displays a table of L2 interfaces counters.

Example

The example below shows the output of the `show interface counters` command:

```
(host) [mynode] #show interface counters
Port          InOctets      InUcastPkts   InMcastPkts
InBcastPkts
GE0/0/0       87071474     45349         590754       112566
Port          OutOctets     OutUcastPkts  OutMcastPkts
OutBcastPkts
GE0/0/0       10646801    18727         581          2
```

The output of this command includes the following parameters:

Parameter	Description
Port	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

Related Commands

Command	Description
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show interface gigabitethernet

show interface gigabitethernet <slot/module/port>

Description

Displays information about a specified Gigabit Ethernet port.

Parameter	Description
access-group	Displays the Access Groups configured on this interface.
counters	Displays L2 interface counters for the specified interface.
switchport	Displays L2 interface information.
transceiver	Displays the transceiver serial ID information.
trusted-vlan	Displays port member vlan trusted status.
untrusted-vlan	Displays port member vlan untrusted status.
xsec	Displays xsec configuration.

Examples

The example below shows the output of `show interface gigabitethernet 0/0/0`:

```
(host)[mynode] (config) #show interface gigabitethernet 0/0/0
GE 0/0/0 is up, line protocol is up
Hardware is 10 Gigabit Ethernet, address is 00:0C:29:37:AB:82 (bia
00:0C:29:37:AB:82)
Description: GE0/0/0
Encapsulation ARPA, loopback not set
speed (10 Gbps)
MTU 1500 bytes, BW is 10000 Mbit
Last clearing of "show interface" counters 5 day 4 hr 57 min 41 sec
link status last changed 5 day 4 hr 55 min 22 sec
1560452 packets input, 498781462 bytes
Received 240098 broadcasts, 0 runts, 0 giants, 0 throttles
0 input error bytes, 0 CRC, 0 frame
240098 multicast, 1320354 unicast
1149614 packets output, 158075706 bytes
0 output errors bytes, 0 deferred
0 collisions, 0 late collisions, 0 throttles
This port is TRUSTED
```

The output of this command includes the following parameters:

Parameter	Description
GE 0/0/0 is...	Displays the status of the specified port.
line protocol is...	Displays the status of the line protocol on the specified port.
Hardware is...	Describes the hardware interface type.
address is...	Displays the MAC address of the hardware interface.
Description	The port type, name, and connector type.
Encapsulation	Encapsulation method assigned to this port.
loopback...	Displays whether or not loopback is set.
Configured	Configured transfer operation and speed.
Jumbo support...	Jumbo frame support is enabled.
Negotiated	Negotiated transfer operation and speed.
MTU bytes	MTU size of the specified port in bytes.
BW is...	Bandwidth of the link.
Last clearing of "show interface counters"	Time since "show interface counters" was cleared.
link status last changed...	Time since "show interface counters" was cleared. Below the time, all current counters related to the specified port are listed.
This port is...	Whether or not this port is trusted.
POE status of the port is...	The POE status of the specified port.
BW-Contract List/ Application Exception List/ Application BW-Contract list	Information about the bandwidth contract applied to the interface. For details, see interface gigabitethernet .

The example below shows the output of `show interface gigabitethernet 0/0/0 counters`:

```
(host)[mynode] (config) #show interface gigabitethernet 0/0/0 counters
Port          InOctets      InUcastPkts   InMcastPkts
InBcastPkts
GE0/0/0      498972448     1321416       240316        0
```

Port	OutOctets	OutUcastPkts	OutMcastPkts
OutBcastPkts GE0/0/0	158234051	1150823	0

The output of this command includes the following parameters:

Parameter	Description
Port	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

The example below shows the output of `show interface gigabitethernet 0/0/0 switchport`:

```
(host)[mynode] (config)#show interface gigabitethernet 0/0/0 switchport

Name: GE0/0/0
Switchport: Enabled
Administrative mode: static access
Operational mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Access Mode VLAN: 1 (Default)
Trunking Native Mode VLAN: 1 (Default)
Trunking Vlans Enabled: NONE
Trunking Vlans Active: NONE
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.

Parameter	Description
Administrative mode	Administrative mode .
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

The example below shows the output of `show interface gigabitethernet 0/0/2 transceiver`:

```
(host)[mynode] (config)#show interface gigabitethernet 0/0/2 transceiver

Module is SFP+
Product Number      : J9151E  HPE
Part Number         : 1990-4727, rev: 10
S/N                 : CN01KBW0FL
Date Code           : 200107 Lot:
Supported Modes     : 10GBASE-LR, LC Connector
Wavelength          : 1310 nm
Aruba Certified     : YES
```

The output of this command includes the following parameters:

Parameter	Description
Module	Indicates the SFP transceiver module.
Product Number	Denotes the product number.
Part Number	Part number provided by the SFP vendor.
S/N	Serial number provided by the SFP vendor.
Date Code	Denotes the vendor's manufacturing date code. It consists of 6 numbers each, two of them represent year, month and day of month respectfully. It also includes a vendor specific lot code which may be blank.

Parameter	Description
Supported Modes	Denotes the transceiver type and the description value.
Wavelength	Displays the wavelength in nm.
Aruba Certified	Displays if the SFP transceiver is certified by Aruba.

The example below shows the output of `show interface gigabitethernet 0/0/0 untrusted-vlan`:

```
(host) [mynode] (config)#show interface gigabitethernet 0/0/0 untrusted-vlan
Name: GE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the specified port.
Untrusted Vlan(s)	List of untrusted VLANs.

The example below shows the output of `show interface gigabitethernet 0/0/1 xsec`:

```
(host) [mynode] (config)# show interface gigabitethernet 0/0/1 xsec
xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
xsec vlan 7 is ACTIVE	This states that xsec is active on the specified port as well as the associated VLAN.

Related Commands

Command	Description
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.

Command	Description
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>Aruba Certified</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show interface list

```
show interface list
```

Description

Lists the interfaces for all platforms supported by current SC version.

Example

```
(host) [mynode] #show interface list

Platforms: A7210, A7220, A7240

interface gigabitethernet 0/0/0
```

```
interface gigabitethernet 0/0/1
interface gigabitethernet 0/0/2
interface gigabitethernet 0/0/3
interface gigabitethernet 0/0/4
interface gigabitethernet 0/0/5
```

Platforms: A9240, A9240_silver

```
interface gigabitethernet 0/0/0
interface gigabitethernet 0/0/1
interface gigabitethernet 0/0/2
interface gigabitethernet 0/0/3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show interface loopback

show interface loopback

Description

Displays information about the loopback IP interface.

Example

The example below shows the output of the `show interface loopback` command:

```
(host) [mynode] #show interface loopback

loopback interface is up line protocol is up
Hardware is Ethernet, address is 00:0C:29:37:AB:81
IPv6 link-local address is fe80::c:290f:ff37:ab81/64
```

The output of this command includes the following parameters:

Parameter	Description
loopback interface is...	Status of the loopback interface.
line protocol is...	Status of the line protocol on the specified port.
Hardware is...	Hardware interface type.
address is...	MAC address of the loopback interface.
IPv6 link-local address	IP address and subnet mask of the loopback interface.

Related Commands

Command	Description
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.

Command	Description
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show interface mgmt

show interface mgmt

Description

Displays information about management Ethernet IP interfaces.

Example

The example below shows the output of `show interface mgmt`:

```
(host) [mynode] (config)# show interface mgmt

mgmt is up line protocol is up
Hardware is Ethernet, address is 00:0C:29:37:AB:77
```

The output of this command includes the following parameters:

Parameter	Description
mgmt is...	Status of the mgmt interface.
line protocol is...	Status of the line protocol on the specified port.
Hardware is...	Describes the hardware interface type.
address is...	Interface's MAC address.

Related Commands

Command	Description
interface mgmt	This command configures the out-of-band Ethernet management port on controller.
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.

Command	Description
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show interface port-channel

```
show interface port-channel <id>
  access-group
  counters
  switchport
  trusted-vlan
  untrusted-vlan
  xsec
    xsec point-to-point
```

Description

Displays information about a specified port-channel interface.

Parameter	Description
access-group	Displays access groups configured on this interface.
counters	Displays L2 interface counters for the specified interface.
switchport	Displays L2 interface information for the specified interface.
trusted-vlan	Displays port member vlan trusted status.
untrusted-vlan	Displays port member vlan untrusted status.
xsec	Displays xsec configuration.
xsec point-to-point	Displays the point-to-point xsec tunnels for the specified interface.

Examples

The examples below show the output of `show interface port-channel 7` on a managed device.

```
(host) [mynode] (config) #show interface port-channel 7
Port-Channel 7 is administratively up, Link is up, Line protocol is down
Hardware is Port-Channel, address is 00:0C:29:37:AB:81 (bia
00:0C:29:37:AB:81)
Description: Link Aggregate
Spanning Tree is Discarding
Switchport priority: 0
Member port(s):
Speed :0 Mbps
Interface index: 8200
MTU: 1500 bytes
Last clearing of "show interface" counters 0 day 8 hr 48 min 3 sec
link status last changed 0 day 8 hr 48 min 3 sec
```



```

0 packets input, 0 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input error bytes, 0 CRC, 0 frame
0 multicast, 0 unicast
0 packets output, 0 bytes
0 output errors bytes, 0 deferred
0 collisions, 0 late collisions, 0 throttles
Port-Channel 7 is NOT TRUSTED

```

The output of this command includes the following parameters:

Parameter	Description
Port-Channel 7 is...	Status of the specified port.
line protocol is...	Status of the line protocol on the specified port.
Hardware is....	Hardware interface type.
address is...	MAC address of the hardware interface.
Description	The port type, name, and connector type. If the LAG is created by LACP, it is indicated as shown in the display output above. If the LAG is created by LACP, you can not statically add or delete any ports under that port channel. All other commands are allowed. If LACP is not shown, then the LAG is created by static configuration.
Spanning Tree is...	Spanning tree status on the specified port-channel.
VLAN membership	Number of VLANs the specified port-channel is associated with.
Switchport priority	Switchport priority of the specified port-channel.
Jumbo Support is...	Displays the status of jumbo frame on a port channel.
Last clearing of "show interface counters"	Time since "show interface counters" was cleared. Below the time, all current counters related to the specified port are listed.
Port-channel 7 is...	Whether or not this port-channel is trusted.

```

Port-Channel 7:

Port-Vlan Session ACL
-----
SessionACL          Vlan      Status
-----          -----

```

The output of this command includes the following parameters:

Parameter	Description
SessionACL	Session ACL name.
Vlan	VLAN number.
Status	ACL status.

```

#show interface port-channel 7 counters
Port          InOctets      InUcastPkts    InMcastPkts    InBcastPkts
PC 0:         0              0              0              0
Port          OutOctets      OutUcastPkts   OutMcastPkts   OutBcastPkts
PC 0:         0              0              0              0

```

The output of this command includes the following parameters:

Parameter	Description
PC	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```

#show interface port-channel 7 trusted-vlan

```

```
Name: Port-channel 7
Switchport: Enabled
Administrative mode: static access
Operational mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Access Mode VLAN: 1 (Default)
Trunking Native Mode VLAN: 1 (Default)
Trunking Vlans Enabled: NONE
Trunking Vlans Active: NONE
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.
Administrative mode	Administrative mode .
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

```
#show interface port-channel 7 trusted-vlan

Name: Port-Channel7
Trusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the specified port.
trusted Vlan(s)	List of trusted VLANs.

```
#show interface port-channel 7 untrusted-vlan

Name: FE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the specified port.
Untrusted Vlan(s)	List of untrusted VLANs.

```
#show interface port-channel 7 xsec

xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
xsec vlan 7 is ACTIVE	This states that xsec is active on the specified port as well as the associated VLAN.

Related Commands

Command	Description
interface mgmt	This command configures the out-of-band Ethernet management port on controller.
interface port-channel	This command configures an Ethernet port channel.
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.

Command	Description
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show interface tunnel

```
show interface tunnel <id> {trusted-vlan | untrusted-vlan}
```

Description

Displays information about tunnel interfaces.

Parameter	Description
id	Tunnel interface number.
trusted-vlan	Displays trusted VLAN list.
untrusted-vlan	Displays untrusted VLAN list.

Examples

The example below shows the output of `show interface tunnel` for IPv4:

```
(host) [mynode] #show interface tunnel 2000

Tunnel stats last fetched from SOS: 8 sec ago
Tunnel 2000 is up line protocol is down
Description: Tunnel Interface
Source 10.16.33.208 (Vlan 33)
Destination 1.1.1.200
Tunnel mtu is set to 1100
Tunnel is a Layer2 GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is enabled
Keepalive type is Default
Tunnel keepalive interval is 1 seconds, retries 1
Heartbeats sent 1992, Heartbeats lost 1991
Tunnel is down 2 times
Trusted vlans:350-850
tunnel vlan 300-900
RxBytes: 0, TxBytes: 384, Encaps: 6, Decaps: 0
```

The example below shows the output of `show interface tunnel` for IPv6:

```
(host) [mynode] #show interface tunnel 20

Tunnel stats last fetched from SOS: 8 sec ago
Tunnel 20 is up line protocol is up
Description: Tunnel Interface
Source 2001:10:16:32::54 (Vlan 32)
```

```

Destination 2001:10:16:32::53
Tunnel mtu is set to 1500
Tunnel is a Layer2 GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is disabled
Keepalive type is Default
Tunnel keepalive interval is 0 seconds, retries 0
Trusted vlan 300-350
tunnel vlan 100,200,300-350
RxBytes: 0, TxBytes: 384, Encaps: 6, Decaps: 0

```

The example below shows the output of `show interface tunnel` for trusted vlan:

```

(host) [mynode] #show interface tunnel 30 trusted-vlan
Trusted Vlan(s):300-350

```

The example below shows the output of `show interface tunnel` for untrusted vlan:

```

(host) [mynode] #show interface tunnel 40 untrusted-vlan
Untrusted Vlan(s):1-299,351-4094

```

The output of this command includes the following parameters:

Parameter	Description
Tunnel stats last fetched from SOS: 8 sec ago	Displays when the tunnel statistics were last fetched from SOS. This parameter is printed only once.
Tunnel 2000 is up line protocol is down	Displays the status of the specified interface tunnel and its line protocol.
Description	Displays the description of the specified interface tunnel.
Source	Displays the IP address of the source of the specified interface tunnel.
Destination	Displays the IP address of the destination of the specified interface tunnel.
Tunnel mtu is set to 1100	Displays the MTU size of the specified interface tunnel.

Parameter	Description
Tunnel is a Layer2 GRE TUNNEL	Displays the layer 2 or layer 3 status of the specified interface tunnel.
Tunnel is trusted	Displays whether or not the specified interface tunnel is trusted.
Inter tunnel flooding is enabled	Displays whether or not the inter tunnel flooding of the specified interface tunnel is enabled.
Tunnel keepalive is disabled	Displays whether or not the tunnel keepalive of the specified interface tunnel is enabled.
Keepalive type is Default	Displays the type of the keepalive of the specified interface tunnel.
Tunnel keepalive interval is 1 seconds, retries 1	Displays the keepalive interval and number of retries configured on the specified interface tunnel.
Heartbeats sent 1992, Heartbeats lost 1991	Displays the number of heartbeats sent and lost on the specified interface tunnel.
Tunnel is down 2 times	Displays the number of times the tunnel was down on the specified interface tunnel.
Trusted vlans:350-850	Displays the VLAN IDs that are trusted on the specified interface tunnel.
tunnel vlan 300-900	Displays the VLAN IDs that are part of the tunnel in the specified interface tunnel.
RxBytes: 0, TxBytes: 384, Encaps: 6, Decaps: 0	Displays the number of sent, received, encapsulated, and decapsulated packets.

Related Commands

Command	Description
interface mgmt	This command configures the out-of-band Ethernet management port on controller.

Command	Description
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>Tunnel stats last fetched from SOS</code> and <code>RxBytes:</code> , <code>TxBytes:</code> , <code>Encaps:</code> , <code>Decaps:</code> parameters were introduced.
ArubaOS 8.4.0.0	The <code>trusted-vlan</code> and <code>untrusted-vlan</code> sub-parameters was introduced in the following command. <ul style="list-style-type: none"> ■ <code>show interface tunnel <id></code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show interface vlan

```
show interface vlan <id> [access-group]
```

Description

Displays information about a specified VLAN interface.

Parameter	Description
<id>	VLAN interface number.
access-group	Session ACL configured on this interface.

Example

The following example displays information about VLAN 20:

```
(host) [mynode] #show interface vlan 20

VLAN20 is up line protocol is up
Hardware is CPU Interface, Interface address is 00:0C:29:3C:F7:D3 (bia
00:0C:29:3C:F7:D3)
Description: 802.1Q VLAN
IPv6 is enabled, link-local address is fe80::c:2900:143c:f7d3
Global unicast address(es):
2017::1, subnet is 2017::/64
IPv6 Router Advertisements are disabled
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled, BCMC Optimization disabled ProxyARP disabled
Suppress ARP enable
Encapsulation 802, loopback not set
MTU 1500 bytes
Last clearing of "show interface" counters 1 day 2 hr 55 min 37 sec
link status last changed 1 day 0 hr 37 min 24 sec
Proxy Arp is disabled for the Interface
IPv6 Helper Addresses Configured on this Interface:
2001:200::1
DHCPv6 relay option is configured on this interface
```

The output of this command includes the following parameters:

Parameter	Description
VLAN1 is...	Status of the specified VLAN.
Line protocol is...	Displays the status of the line protocol on the specified port.

Parameter	Description
Hardware is...	Describes the hardware interface type.
Interface address is...	Displays the MAC address of the hardware interface.
Description	Description of the specified VLAN.
Internet address is...	IP address and subnet mask of the specified VLAN.
IPv6 Router Advertisements...	Status of IPv6 RA.
Routing interface is...	Status of the routing interface.
Forwarding mode is...	Status of the forwarding mode.
Directed broadcast is...	Displays whether or not directed broadcast is enabled.
BCMC Optimization...	Status of broadcast-multicast optimization.
ProxyARP...	Status of proxy ARP. Proxy ARP is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network.
Supress ARP...	Status of suppressed ARP. If enabled, the managed device prevents flooding of ARP broadcasts on all the untrusted interfaces.
Encapsulation	Encapsulation type.
Loopback...	Loopback status.
MTU	MTU size of the specified port in bytes.
Last clearing of "show interface counters"	Time since show interface counters was cleared.
link status last changed	Time since link status last changed.
Proxy ARP is...	Status of proxy ARP on the specified interface.
IPv6 Helper Addresses...	Helper address configured for a vlan.

Related Commands

Command	Description
interface mgmt	This command configures the out-of-band Ethernet management port on controller.

Command	Description
interface range	This command configures a range of GigabitEthernet interfaces on the managed device.
interface tunnel	This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.
interface vlan	This command configures a VLAN interface.
interface vlan ip igmp	This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Command History

Release	Modification
ArubaOS 8.2.0.0	The IPv6helper-address was displayed in the output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show inventory

show inventory

Description

This command displays the hardware inventory of Mobility Conductor or the managed device.

Example

Execute this command to display the hardware component inventory of Mobility Conductor.

```
(host) [mynode] #show inventory

Mgmt Port HW MAC Addr      : 00:0C:29:71:10:0B
HW MAC Addr                 : 00:0C:29:71:10:15
System Serial#             : DC0604083
Activate license            : Not applicable
Supported device type      : MM
Active device type         : MM
```

Issue this command to display the hardware component inventory of the managed device. The output of this command will vary depending on the controller platform type.

```
(host-md) #show inventory

Supervisor Card slot       : 0
System Serial#            : BA0009743 (Date:12/26/14)
CPU Card Serial#          : AE51038711 (Date:12/25/14)
CPU Card Assembly#        : 2010216H
CPU Card Revision          : (Rev:01.00)
Interface Card Serial#     : AE51031572 (Date:12/25/14)
Interface Card Assembly#   : 2010085E
Interface Card Revision    : (Rev:04.00)
SC Model#                 : Aruba7210
HW MAC Addr               : 00:1a:1e:01:b2:28 to 00:1a:1e:01:b2:2f
CPLD Version              : (Rev: 1.4)
Power Supply 0             : Present           : No
Power Supply 1             : Present           : Yes
: 12V OK                   : Yes
: Fan OK                    : Yes
: Aruba Model No           : 2510057
: Vendor & Model No        : QCS DCJ3501-01P
: Serial No                : QCS142320YU
: MFG Date                 : 6/5/14
: Output 1 Config          : 12V 350W
: Input Min                 : 90V AC
: Input Max                 : 264V AC
Main Board Temperatures   :
: U24 - Local Temp        : 30 C (shadow of XLP heatsink)
```

```

: Q1 - Remote 1 Temp      34 C (shadow of VRM, VDD_CPU)
: Q2 - Remote 2 Temp      33 C (shadow of VRM, VDD_SOC)
: U44 - Local Temp        25 C (shadow of DFI connector)
: U29 - Remote 1 Temp     31 C (XLP die temperature)
: Q36 - Remote 2 Temp     28 C (shadow of 98X1422)
: J2 - DDR A Temp         24 C (DDR3 A temp)
: J4 - DDR B Temp         26 C (DDR3 B temp)
: J1 - DDR C Temp         25 C (DDR3 C temp)
: J3 - DDR D Temp         27 C (DDR3 D temp)
: Port 0 Temp             148 C (1G PHY temp)
: Port 1 Temp             148 C (1G PHY temp)
Interface Board Temperatures :
: U21 - Local Temp        27 C (shadow of port 1 RJ45)
: Q4 - Remote 1 Temp      28 C (shadow of 88E1543)
: Q3 - Remote 2 Temp      34 C (shadow of 88X2140)
Fan 0                     : 8916 rpm (5.495 V), Speed Low
Fan 1                     : 9029 rpm (5.495 V), Speed Low
Fan 2                     : 9029 rpm (5.450 V), Speed Low
Fan 3                     : 8998 rpm (5.630 V), Speed Low
Main Board Voltages       :
ispPAC_POWR1014A_A       :
: 1V2                    1.20V sense 1.232 V
: VDD SOC                 0.937V sense 0.918 V
: VCC IOBD 1V5           1.50V sense 1.528 V
: DDR3BD_VTT             0.75V sense 0.750 V
: VCC 1A                 1.00V sense 1.024 V
: IV8_DIGITAL            1.80V sense 1.848 V
: 3V3_MAIN               3.30V sense 3.366 V
: VCC1                   1.00V sense 1.018 V
: VCC25                  2.50V sense 2.556 V
: 3V3 SB                 3.30V sense 3.360 V
ispPAC_POWR1014A_B       :
: VDD                    0.806V sense 0.786 V
: VCC IOAC 1V5           1.50V sense 1.528 V
: DDR3AC_VTT             0.75V sense 0.752 V
: VDD_SRAM               1.00V sense 1.042 V
: VCC1B                  1.00V sense 1.030 V
: 1V8_ANALOG             1.80V sense 1.854 V
: 1V8                    1.80V sense 1.866 V
: VDDIO12_XAUI          1.20V sense 1.224 V
: 5V                     5.00V sense 5.016 V
Interface Board Voltages  :
ispPAC_POWR6AT6         :
: VCC33                  3.30V sense 3.366 V
: VCC 18                 1.80V sense 1.856 V
: VCC1                   1.00V sense 1.026 V
: VCC12                  1.20V sense 1.224 V
: VCC12-DVDD            1.20V sense 1.212 V
: VCC9                   0.90V sense 0.928 V

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor and Enable mode on Managed Device.

show iot

```
show iot
  manager
  transportProfile
  radio-profile
  iostat
```

Description

This command displays the list of all interfaces. Click the parameter links below to view the corresponding show commands.

Parameter	Description
manager	Displays the status of the IoT manager.
transportProfile	Displays the list of IoT transport profiles and the context and status of the IoT transport profiles.
radio-profile	Displays the list of IoT radio profiles and the context and status of the IoT radio profiles.
iostat	Displays Input/Output statistics information. This command reports Central Processing Unit (CPU) statistics and Input/Output statistics for devices and partitions.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

Parameter	Description
swap	The number of swap pages that have been brought in and out.
intr	The number of interrupts received from the system boot.
disk_io	(x,y) is (major, minor):(xx, xx, xxxx, x, x) is (noinfo, read_io_ops, blks_read, write_io_ops, blks_written).
ctxt	The number of context switches that the system underwent.
btime	The boot time, in seconds.
processes	The number of forks since boot.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show iot radio-profile

```
show iot radio-profile [<profile-name>]
```

Description

This command displays the list of IoT radio profiles and the context and status of the IoT radio profiles.

Examples

The following example shows the list and context of IoT transport profiles:

```
(host) [mynode] #show iot radio-profile

IoT Radio Profile List
-----
Name                References  Profile Status
-----
Sample-Ble          0
Sample-Zigbee       0

Total: 2
```

The following example shows the status of an IoT radio profile:

```
(host) [mynode] #show iot transportProfile Sample-Zigbee

IoT Data Profile "Sample-Zigbee"
-----
Parameter                Value
-----
Radio Instance            internal
Radio Mode                zigbee
Radio Enable              Enabled
ZipBee Opmode             coordinator
ZipBee Channel            auto
ZipBee Permit Joining    on
ZipBee Permit Joining Duration 300
ZipBee PAN ID Type       auto
ZipBee PAN ID             0000
```

Related Commands

Command	Description
iot radio-profile	This command configures an IoT radio profile.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show iot transportProfile

```
show iot transportProfile [<profile-name>]
```

Description

This command displays the list of IoT transport profiles and the context and status of the IoT transport profiles.

Examples

The following example shows the list and context of IoT transport profiles:

```
(host) [mynode] #show iot transportProfile

IoT Data Profile List
-----
Name                               References  Profile Status
-----
iot_xg_assettag                    0
iot_xg_assettag_staging            0
test                                0

Total: 3
```

The following example shows the status of an IoT transport profile:

```
(host) [mynode] #show iot transportProfile test

IoT Data Profile "test"
-----
Parameter                           Value
-----
Server Type                           Telemetry-Websocket
Server URL                             N/A
Access Token                           N/A
Client Id                              N/A
Username                               N/A
Password                               N/A
Reporting interval                     600
Device Class Filter                    exposure-notification
UUID Filter                            N/A
Movement Filter                        0
Cell Size Filter                       0
Vendor Filter                          N/A
Age Filter                             0
Authentication URL                     N/A
UID Namespace Filter                   N/A
URL Filter                             N/A
Access ID                              N/A
```

```

Zigbee Socket Device Filter N/A
RSSI Reporting Format average
choose an environment type office
Custom Fading Factor 20
Iot Proxy Server 192.168.1.1 8087
Iot Proxy User admin *****
AP Group N/A
Send device counts only Disabled
RTLS Destination MAC Address N/A
Data Filter N/A

```

Related Commands

Command	Description
iot transportProfile	This command configures an IoT transport profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	<p>The following parameters were introduced:</p> <ul style="list-style-type: none"> ■ Zigbee Socket Device Filter ■ Data Filter <p>The following deviceClassFilter were introduced:</p> <ul style="list-style-type: none"> ■ exposure-notification ■ wiliot ■ ZSD <p>The Enable BLE on Controller parameter was removed.</p>
ArubaOS 8.6.0.0	The Vendor Filter, IoT Proxy Server, IoT Proxy User, Send device counts only, and RTLS Destination MAC Address parameters were introduced.
ArubaOS 8.5.0.0	The aruba-sensors sub-parameter was introduced under the Device Class Filter parameter.
ArubaOS 8.4.0.0	<p>The following parameters were renamed:</p> <ul style="list-style-type: none"> ■ Endpoint Type to Server Type ■ Endpoint URL to Server URL ■ Server Token to Access Token ■ Endpoint ID to Client Id

Release	Modification
	<ul style="list-style-type: none"> ■ Endpoint Username to Username ■ Endpoint Password to Password ■ AP data transport interval to Reporting interval ■ IoT payload content to Device Class Filter ■ Filter Attributes to UUID Filter ■ Threshold Attributes to Movement Filter <p>The following parameters were added:</p> <ul style="list-style-type: none"> ■ Cell Size Filter ■ Age Filter ■ Authentication URL ■ UID Namespace Filter ■ URL Filter ■ RSSI Reporting Format ■ choose an environment type ■ Custom Fading Factor ■ AP Group
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show iot-manager

```
Show iot-manager
  ble-services ibeacon-info [ap-group <ap-group>] [ble-profile <ble-profile>]
  debug db-dump-status
  debug db-optimize-status
  log level
```

Description

This command shows the status of the IoT manager.

Parameter	Description
ble-services ibeacon-info	This parameter shows the iBeacon information of devices.
ap-group <ap-group>	This parameter filters the iBeacon information of devices by the ap-group.
ble-profile <ble-profile>	This parameter filters the iBeacon information of devices by the BLE profile.
debug db-dump-status	This parameter shows the database dump status information.
debug db-optimize-status	This parameter shows the database optimization status information.
log	This parameter shows the logs from IoT manager process.

Examples

Access the CLI and use the following command to show the status of the IoT manager:

```
(host) [mynode] #show iot-manager debug db-dump-status

IM DB dump status
-----
Field          Value
-----
Status:        Success
Filename:      im_db_dump.tgz
Begin Time:    2019-04-30 06:47:48
End Time:      2019-04-30 06:47:48
```

Access the CLI and use the following command to show the status of the IoT manager:


```
(host) [mynode] #show iot-manager ble-service ibeacon-info profile default

AP's BLE radio iBeacon parameter
-----
AP Eth MAC          BLE MAC          Radio instance Major  Minor  UUID
-----
38:17:c3:c0:c8:ba  7c:01:0a:ff:22:22 internal 1000  1000  4152554E-F99B-
4A3B-86D0-947070693A78

Total AP BLE devices reported: 1
```

Related Commands

Command	Description
iot-manager	This command configures the IoT manager settings.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>ble-services</code> parameter was added.
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show ip

```
show ip
  access-group
  access-list
  cp-redirect-address
  dhcp
  domain-name
  dynamic-dns
  health-check
  igmp
  interface
  mobile
  nat
  nexthop-list
  ospf
  pppoe-info
  probe
  radius
  route
  tacacs
```

Description

Displays IP related details.

Parameter	Description
<u>access-group</u>	Displays ACLs configured for each port on Mobility Conductor.
<u>access-list</u>	Displays a table of all configured ACLs, or show details for a specific ACL.
<u>cp-redirect-address</u>	Show the captive portal automatic redirect IP address.
<u>dhcp</u>	Displays the DHCP server binding, database setting, relay and pool statistics.
<u>domain-name</u>	Displays the full domain name and server.
<u>dynamic-dns</u>	Displays the dynamic DNS details.
<u>health-check</u>	Displays the health-check status of the uplink interfaces of a branch office managed device.
<u>igmp</u>	Displays IGMP timers and counters.
<u>interface</u>	IP interface information

Parameter	Description
mobile	Displays statistics and configuration information for the mobile protocol.
nat	Displays a pool of IP addresses for NAT.
nexthop-list	Displays the next hop list settings for policy-based routing. A next hop IP is the IP address of a adjacent router or device with layer-2 connectivity to managed device.
ospf	Displays statistics and configuration information for the OSPF routing protocol.
pppoe-info	Displays the configuration settings for PPPoE.
probe	Displays the health-check profile settings for measuring WAN reachability and latency on a managed device uplink, and the default probe profile settings for PBR using next-hop lists.
radius	Displays global parameters for configured RADIUS servers.
route	Displays the Mobility Conductor routing table with static routes configured on the Mobility Conductor using the ip route command.
tacacs	Displays global parameters for configured TACACS servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip access-group

show ip access-group

Description

Displays ACLs configured for each port on Mobility Conductor.

Examples

The example below shows part of the output of this command. If a port does not have a defined session ACL, the *Port-Vlan Session ACL* table will be blank.

```
(host) [mynode] #show ip access-group

FE 1/0:
Rx access list 200 is applied
session access list User14 is applied

Port-Vlan Session ACL
-----
SessionACL          Vlan      Status
-----
coltrane             22        configured
```

The output of this command includes the following parameters:

Parameter	Description
Session ACL	Name of the ACL applied to the interface.
VLAN	If the ACL was applied to a VLAN associated with this port, this column will show the VLAN ID.
Status	Shows whether or not the session ACL is configured.

Related Commands

Command	Description
ip access-group	Configures an access group for an interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip access-list

```
show ip access-list
  brief [ipv4|ipv6]
  <string>
  global-geolocation-acl
```

Description

This command displays a table of all configured ACLs, or show details for a specific ACL.

Parameter	Description
brief	Display a table of information for all ACLs.
<string>	Specify the name of a single ACL to display detailed information on that ACL.
global-geolocation-acl	Displays configured values of the global-geolocation-acl ACL.

Examples

The example below shows general information for all ACLs in the Access List table.

```
(host) [mynode] #show ip access-list brief

Access list table (4 - IPv4, 6 - IPv6)
-----
Name                               Type                Use Count  Roles
----                               -
allow-diskservices                 session(4)
allow-printservices                session(4)
allowall                           session(46)         3          default-via-role
default-vpn-role authenticated
ap-acl                             session(4)          1          ap-role
ap-uplink-acl                     session(4)
apprf-authenticated-sacl           session             1          authenticated
apprf-default-via-role-sacl        session             1          default-via-role
apprf-default-vpn-role-sacl        session             1          default-vpn-role
apprf-guest-sacl                   session             1          guest
apprf-stateful-dot1x-sacl          session             1          stateful-dot1x
apprf-voice-sacl                   session             1          voice
captiveportal                      session(4)          2          guest-logon logon
captiveportal6                     session(6)          2          guest-logon logon
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of an ACL.
Type	Shows that the ACL is one of the following ACL policy types: <ul style="list-style-type: none"> ■ Ethertype ■ Standard ■ Session ■ MAC ■ Extended
Use Count	Number of rules defined in the ACL.
Roles	Names of user roles associated with the ACL.

Include the name of a specific ACL to show detailed configuration information for that ACL. The output in the example below has been divided into two sections to better fit into this document. The output in the CLI will appear in a single, long table.

```
(host) [mynode] # show ip access-list captiveportal6

ip access-list session captiveportal6
captiveportal6
-----
Priority Source Destination Service Application Action NextHopList TimeRange
-----
1 user md-6 svc-https captive
2 user any svc-http captive
3 user any svc-https captive
4 user any svc-http-proxy1 captive
5 user any svc-http-proxy2 captive
6 user any svc-http-proxy3 captive

Log Expired Queue TOS 8021P Blacklist
/Denylist
Mirror DisScan IPv4/6 Contract
---
Low 6
Low 6
Low 6
Low 6
Low 6
Low 6
```

The following parameters are used specifically for the bridge mode:

```
show ip access-list captiveportalbridge
show ip access-list logon-control-bridge
```

The output of the `show ip access-list` command may include some or all of the following parameters:

Parameter	Description
Priority	Name of an access-control list (ACL).
Source	<p>The traffic source, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ alias: The network resource (use the <code>netdestination</code> command to configure aliases; use the <code>show netdestination</code> command to see configured aliases) ▪ any: Matches any traffic. ▪ host: A single host IP address. ▪ network: The IP address and netmask. ▪ user: The IP address of the user. ▪ localip: The set of all local IP addresses on the system, on which the ACL is applied.
Destination	<p>The traffic destination, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ alias: The network resource (use the <code>netdestination</code> command to configure aliases; use the <code>show netdestination</code> command to see configured aliases) ▪ any: Matches any traffic. ▪ host: A single host IP address. ▪ network: An IP address and netmask. ▪ user: The IP address of the user. ▪ localip: The set of all local IP addresses on the system, on which the ACL is applied.
Service	<p>Network service, which can be one of the following:</p> <ul style="list-style-type: none"> ▪ An IP protocol number (0-255). ▪ The name of a network service (use the <code>show netservice</code> command to see configured services). ▪ any: Matches any traffic. ▪ tcp: A TCP port number (0-65535). ▪ destination port number: specify the TCP port number (0-65535) ▪ source: TCP or UDP source port number ▪ udp: A UDP port number (0-65535).

Parameter	Description
Application	Name of the application to which the ACL is applied. (For a complete list of supported applications, issue the command <code>show dpi application all</code> .)
Action	Action if rule is applied, which can be one of the following: <ul style="list-style-type: none"> ▪ deny: Reject packets. ▪ dst-nat: Perform destination NAT on packets. ▪ dual-nat: Perform both source and destination NAT on packets. ▪ permit: Forward packets. ▪ redirect: Specify the location to which packets are redirected, which can be one of the following: <ul style="list-style-type: none"> ◦ Datapath destination ID (0-65535). ◦ esi-group: Specify the ESI server group configured with the <code>esi group</code> command ◦ opcode: Specify the datapath destination ID (0x33, 0x34, or 0x82). Do not use this parameter without proper guidance from Aruba. ▪ tunnel: Specify the ID of the tunnel configured with the <code>interface tunnel</code> command. ▪ src-nat: Perform source NAT on packets.
IpssecMap	Packets can be redirected over a VPN tunnel by specifying the name of an IPsec map in the ACL. This column specifies the name of an IPsec map used by a router ACL. For more information on IPsec maps, see crypto-local ipsec-map .
Timerange	Any defined time range for this rule.
NextHopList	If the access rule uses PBR to forwards packets to a nexthop device, then this column displays the next-hop list associated with the rule. For more information on next-hop lists, see ip nexthop-list on page 871 .
Tunnel	Packets can be redirected over an L3 GRE tunnel. If the ACL routes packets over a tunnel, this column specifies the tunnel used by the ACL.
TunnelGroup	Packets can be redirected over an L3 GRE tunnel group. If the ACL routes packets over a tunnel in a tunnel group, this column specifies the tunnel group used by the ACL. For more information on tunnel groups, see tunnel-group .
Log	Shows if the rule was configured to generate a log message when the rule is applied.
Expired	Shows if the rule has expired.

Parameter	Description
Queue	Shows if the rule assigns a matching flow to a priority queue (high or low).
8021.p	802.11p priority level applied by the rule (0-7).
Blacklist/Denylist	Shows if the rule should blacklist/denylist any matching user.
Mirror	Shows if the rule was configured to mirror all session packets to datapath or remote destination.
DisScan	Shows if the rule was configured to pause ARM scanning while traffic is present.
IPv4/6	Shows the IP version.
Contract	Shows the bandwidth contract status.

Related Commands

Command	Description
ip access-list session	Configure an access list for an interface.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.7.0.0	The following parameters were introduced for VAPs in the bridge mode: <ul style="list-style-type: none"> ▪ <code>captiveportalbridge</code> ▪ <code>logon-control-bridge</code> The <code>global-geolocation-acl</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip cp-redirect-address

show ip cp-redirect-address

Description

Show the captive portal automatic redirect IP address.

Examples

The example below shows the IP address to which captive portal users are automatically directed.

```
(host) [mynode] # show ip cp-redirect-address  
  
Captive Portal IPv4 redirect Address ... 10.3.63.11  
Captive Portal IPv6 redirect Address ... ::1
```

Related Commands

Command	Description
ip cp-redirect-address	This command configures a redirect address for captive portal.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip dhcp

```
show ip dhcp
  binding
  database
  option-82
  relay counters
  reserved
  statistics
  vlan
```

Description

This command displays the DHCP server binding, database setting, relay, pool statistics, and device reservations.

Parameter	Description
binding	Show DHCP server bindings.
failover-peer	Show DHCP server failover peer bindings.
ip-address	Show DHCP server binding for IP address.
mac-address	Show DHCP server bindings.
database	Show DHCP server settings.
option-82	Show DHCP option-82 configurations.
relay counters	Show DHCP relay information.
reserved	Show DHCP server device reservations.
statistics	Show DHCP pool statistics.
vlan	Show DHCP vlan information.

Examples

The following example displays DHCP statistics for two configured networks:

```
(host) [mynode] #show ip dhcp statistics

DHCPv4 enabled; DHCPv6 enabled
DHCP Pools
-----
```

Network Name	Type	Active	Configured leases	Active leases	Free leases
2-2-2-nw	v4	Yes	242	0	242
3-2-2-nw	v4	Yes	254	0	254
test	v4	Yes	254	0	254
2011	v6	No	5	-	-
2012	v6	No	5	-	-
Current leases		750			
Total leases		512			

Starting from ArubaOS 8.2.0.0, if the DHCP lease limit is configured to exceed the user limit, a warning is displayed in the command output.

```

host) (config) #show ip dhcp statistics
DHCPv4 disabled; DHCPv6 disabled
DHCP Pools
-----
Network Name  Type  Active  Configured leases  Active leases  Free leases
Expired leases
-----
Abandoned leases
-----
Current leases      0
Total leases      2048
WARNING: DHCP lease limit increased beyond user limit. Some of the controller's services may be impacted
NOTE: To make a DHCPv6 pool active, ensure that the pool name is added in
vlan interface.

```

The output of this command includes the following parameters:

Parameter	Description
Network Name	Range of addresses that the DHCP server may assign to clients.
Type	Indicates the IP version of the DHCP server. It can be v4 or v6.
Active	Indicates if the DHCP server is active or not.
Configured leases	Number of leases configured on the DHCP server.

Parameter	Description
Active leases	Number of active DHCP leases.
Free leases	Number of available DHCP leases.
Expired leases	Number of leases that have expired because they have extended past their valid lease period.
Abandoned leases	Number of abandoned leases. Abandoned leases will not be reassigned unless there are no free leases available.

The following example displays information about DHCP server device reservations:

```
(host) [mynode] (config) #show ip dhcp reserved
DHCP Server Device Reservation Information
-----
Hardware Address  Reserved IP Address  Hostname  Lease Status
-----
00:1A:1E:C0:80:28  10.3.129.253
00:0B:86:42:35:80  10.3.129.99
00:1A:1E:C0:1C:60  10.3.129.254        print    CONNECTED
```

The output of this command includes the following parameters:

Parameter	Description
Hardware Address	Indicates the MAC address of the client device.
Reserved IP Address	Indicates the IP addresses manually reserved from a DHCP pool.
Hostname	Indicates the hostname of the client device.
Lease Status	Indicates whether the client received the IP address or not. This parameter displays one of the following values: <ul style="list-style-type: none"> ■ Connected ■ Disconnected <p>NOTE: The Lease Status displays Connected after a successful DHCP negotiation, when the client receives an IP address from the reserved list. The Lease Status displays Disconnected when the IP address is not assigned to the client.</p>

Related Commands

Command	Description
ip dhcp pool	This command configures a DHCP pool on Mobility Conductor.
ipv6 dhcp pool	This command configures a DHCPv6 pool on Mobility Conductor.
ip dhcp increase-lease-limit	This command increases the DHCP scope on a controller—7005, 7008, or 7010 controllers—to twice the user limit.
ip dhcp reserved	This command configures DHCP server device reservations.

Command History

Release	Modification
ArubaOS 8.8.0.0	The reserved parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip domain-name

```
show ip domain-name
```

Description

This command displays the full domain name and server.

Examples

The following example displays that the IP domain lookup feature is enabled, and the DNS server is configured on the managed device.

```
(host) [mynode] #show ip domain-name

IP domain lookup:           Enabled
IPv6 domain lookup:        Enabled
IP Host.Domain name:       SP-VMC.
IP Domain Redirect:        Enabled
DNS servers
=====
10.13.6.110
10.13.5.200
2020::abcd:abcd

Redirect DNS servers
=====
xyzcorp.com.....         192.168.11.2
xyzcorp.com.....         2001:0000::1101
```

Related Commands

Parameter	Description
ip domain-name	This command configures the default domain name.
ip domain redirect	This command enables the DNS redirect for hostname translation.
ip domain redirect	This command configures the DNS and IP address to be redirected.
ipv6 domain-redirect	This command configures the DNS and IPv6 address to be redirected.
ipv6 domain lookup	This command enables IPv6 Domain Name System hostname translation for clients.

Parameter	Description
ipv6 name-server	This command configures the IPv6 address of the domain name server.
ip dhcp pool	This command configures a DHCP pool on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.4.0.0	The following commands were introduced. <ul style="list-style-type: none"> ▪ ip domain redirect ▪ ip domain-redirect ▪ ipv6 domain-redirect
ArubaOS 8.2.0.0	The IPv6 domain lookup parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip dynamic-dns info

```
show ip dynamic-dns info
```

Description

This command displays the dynamic DNS details.

Example

The following command displays the dynamic DNS details,

```
(host)[mm]show ip dynamic-dns info
DDNS CONFIG
-----
DDNS Status      :      Enabled
DDNS Server      :      10.8.218.119
DDNS Key         :      hmac-md5:arubaddnsmd5.:De+6P2vv6W3KzbfPmkYDpQ==
DDNS Interval    :      86400 seconds
DDNS Enabled DHCP Pools
-----
vlan_60
vlan_192
```

Related Commands

Command	Description
ip dynamic-dns	This command configures DDNS information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip health-check

```
show ip health-check <probe-ip> <src_intf>
```

Description

This command displays the health-check status of the uplink interfaces of a branch office managed device. This command must be executed from the branch office managed device.

Parameter	Description
debug	Displays health-check debug information.
nhinfo	Displays uplink nexthop information.
proberef	Displays uplink probe profile reference list.
verbose	Displays detailed statistics for IP health-check information.
<probe-ip>	IP address of Mobility Conductor.
<src_intf>	Source interface VLAN.

Example

The following example displays the status of two uplinks on a branch office managed device.

```
(host-md) #show ip health-check

IP Health-check Entries
-----

Probe IP          Src Interface  Vpnc IP      State  Probe-Profile
Latency(ms)      Jitter  Loss(%)      MOS
-----
-----
9.9.9.9           vlan 4093                Up    health-check-default
44.400           0
5.5.5.21         vlan 4093      182.72.28.53  Up    data-vpnc
10.000           0.000  0             4.4
10.17.126.161                0             Up    default
0.000
-----
Total Entries: 3
```

The output of this command includes the following data columns.

Parameter	Description
Probe IP	IP address of Mobility Conductor.
Src Interface	IP address of the uplink gateway interface through which the probes were sent.
VPNC IP	Displays the VPN client IP address.
State	Displays the uplink state as either UP or DOWN.
Probe-Profile	Displays the name of the IP probe profile. For information on configuring an IP probe profile, see ip probe default
Latency (ms)	Displays the latency in ms. Latency is calculated based on the delay of ping responses.
Jitter	Displays the jitters in packet flow. Jitter is a variation in the delay of received packets, which can be worsened by network congestion, improper queuing and configuration errors.
Loss (%)	Displays the data packet loss in percentage.
MOS	Displays the estimated Mean Opinion Score.

Related Commands

Command	Description
ip probe default	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.
show ip probe	This command displays the settings for the WAN health-check ping-probes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ip igmp

```
show ip igmp
  cluster
  config
  counters
  group maddr <maddr> [mac <mac-addr>|source <addr>]
  interface [vlan <vlan>]
  proxy-group [vlan <vlan>]
  proxy-mobility-group maddr <maddr>
  proxy-mobility-stats
  proxy-stats
```

Description

This command displays IGMP timers and counters.

Parameter	Description
cluster	See show ip igmp cluster .
config	Show the current IGMP configuration
counters	Display a list counters for the following IGMP queries: <ul style="list-style-type: none">received-totalreceived-queriesreceived-v1-reportsreceived-v2-reportsreceived-leavesreceived-unknown-typeslen-errorschecksum-errorsnot-vlan-drtransmitted-queriesforwarded
group maddr <maddr>	Displays the following IGMP group information: <ul style="list-style-type: none">mac: Specify MAC address of the specific member.source: Specify the source address of the specific SSM group.
interface vlan <vlan>	Show IGMP interface information
proxy-group vlan <vlan>	Show IGMP proxy group information for a specific interface.

Parameter	Description
proxy-mobility-group maddr <maddr>	Display the IGMP proxy group information stored for mobile clients which are away from the managed device.
proxy-mobility-stats	Display the most important messages exchanged between the mobility process and the IGMP proxy.
proxy-stats	Display the number of messages transmitted and received by the IGMP proxy on the upstream interface

Examples

The following example displays the IGMP interface table for all VLANs on Mobility Conductor.

```
(host) [mynode] #show ip igmp interface vlan 2

IGMP Interface Table
-----
VLAN  Addr          Netmask          MAC Address      IGMP      Snooping
Querier  Destination IGMP Proxy
----  -
64    10.6.4.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled
10.6.4.252 CP          disabled
65    10.6.5.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled
10.6.5.252 CP          disabled
1    10.6.2.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled
10.6.2.252 CP          disabled
66    10.6.6.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled
10.6.6.252 CP          disabled
63    10.6.3.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled
10.6.3.252 CP          disabled
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	A VLAN ID number.
Addr	IP address of a VLAN router.
Netmask	Subnet mask for the IP address.
MAC Address	MAC destination address.
IGMP	Indicates if IGMP is enabled (or disabled) on the interface.
Snooping	Indicates if IGMP snooping is enabled (or disabled).

Parameter	Description
Querier	IP address of an IGMP querier.
Destination	Traffic destination.
IGMP Proxy	Indicates if IGMP proxy is enabled (or disabled).

The following example displays the current IGMP configuration settings for Mobility Conductor.

```
(host) [mynode] #show ip igmp config

IGMP Config
-----
Name                               Value
----                               -
robustness-variable                2
query-interval                     30
query-response-interval            100
startup-query-interval             31
startup-query-count                2
last-member-query-interval         10
last-member-query-count            2
version-1-router-present-timeout   400
version-2-router-present-timeout   400
max-members-per-group              300
quick-client-convergence            enabled
ssm-range                          IANA standard range. 232.0.0.0/8
```

The output of this command includes the following parameters:

Parameter	Description
robustness-variable	This variable is increased from its default level of 2 to allow for expected packet loss on a subnetwork.
query-interval	Interval, in seconds, at which Mobility Conductor sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.
query-response-interval	Maximum time, in .1 second intervals, that can elapse between when Mobility Conductor sends a host-query message and when it receives a response. This must be less than the <code>query-interval</code> .
startup-query-count	Number of queries that Mobility Conductor sends out on startup, separated by <code>startup-query-interval</code> . The default setting is the value of the <code>robustness-variable</code> parameter.

Parameter	Description
startup-query-interval	Interval, in seconds, at which Mobility Conductor sends general queries on startup. The default value of this parameter is 1/4 of the query-interval.
last-member-query-count	Number of group-specific queries that Mobility Conductor sends before assuming that there are no local group members.
last-member-query-interval	Maximum time, in seconds, that can elapse between group-specific query messages.
version-1-router-present-timeout	Timeout, in seconds, if Mobility Conductor detects a version 1 IGM router.
version-2-router-present-timeout	Timeout, in seconds, if Mobility Conductor detects a version 2 IGM router.

The following examples displays the information on IGMP groups:

```
(host) [mynode] #show ip igmp group

IGMP Group Table
-----
(Source,Group)          Members
-----
(172.12.2.2, 232.0.0.2) 2
(172.12.2.2, 232.0.0.1) 2
(*, 224.0.0.252)        2
(*, 239.255.255.250)    2

Total Groups: 4

(host) [mynode] #show ip igmp group maddr 232.0.0.1 source 172.12.2.2

IGMP Group (172.12.2.2, 232.0.0.1) Table
-----
Member          MAC              Vlan  Destination  Version  Age
-----
172.13.0.4      00:00:00:00:00:00  13    0/0/0        0        4
172.12.255.252  98:fc:11:c6:20:04  13    Tunnel 9     3        4
```

Related Commands

Command	Description
ip igmp	This command configures IGMP timers and counters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip igmp cluster

```
show ip igmp cluster
  aac-info
  bss-info
  client-info
  dmo-off-info
  info
  proxy-group
  stats
```

Description

Display IGMP related cluster information.

Parameter	Description
aac-info	Show Cluster AAC information of APs.
bss-info	Show IGMP BSS information.
client-info	Show IGMP cluster client information.
dmo-off-info	Show list of (S,G,BSS) where DMO threshold is hit.
info	Show Cluster information.
proxy-group	Show IGMP cluster proxy database group information.
stats	Show cluster statistics.

Related Commands

Command	Description
ip igmp	This command configures IGMP timers and counters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on managed device.

show ip interface brief

```
show ip interface brief
```

Description

This command displays the IP-related information on all interfaces in summary format.

Example

```
(host) #show ip interface brief
Interface                IP Address / IP Netmask      Admin  Protocol
VRRP-IP
vlan 1                   172.16.0.254 / 255.255.255.0  up     up
vlan 2                   10.4.62.9 / 255.255.255.0    up     up
loopback                 unassigned / unassigned      up     up
mgmt                    unassigned / unassigned      down   down
```

The following table details the columns and content in the show command.

Column	Description
Interface	List the interface and interface identification, where applicable.
IP Address /IP Netmask	List the IP address and netmask for the interface, if configured.
Admin	States the administrative status of the interface. Enabled—up Disabled—down
Protocol	Status of the IP on the interface. Enabled—up Disabled—down
VRRP-IP	VRRP IP address associated to the interface.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show ip mobile

```
show ip mobile
  act
  active-domains
  binding [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
  domain [<name>]
  global
  hat
  host [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
  multicast-vlan-table [client-macaddr]
  packet-trace [<count>]
  remote <host-ip>|<host-ipv6>|<host-macaddr>
  trace <host-ip>|<host-ipv6>|<mac-addr>|{force <host-ip>|<host-ipv6>|<mac-addr>}
  traffic dropped|foreign-agent|home-agent|proxy
  trail <host-ip>|<host-ipv6><host-macaddr>
  tunnel
  visitor [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
```

Description

This command displays statistics and configuration information for the mobile protocol.

Parameter	Description
act	Active anchor managed device table; subnets to another managed device map.
active domains	IP mobility domains active on this switch
binding	Display a list of Home Agent Bindings
[<host-ip>]	Filter the Home Agent Bindings list to display data for a specific host IPv4 address.
[<host-ipv6>]	Filter the Home Agent Bindings list to display data for a specific host IPv6 address.
[<host-macaddr>]	Filter the Home Agent Bindings list to display data for a specific host MAC address.
[brief]	Limit the output of this command to show just two lines of data.
domain [<name>]	Display subnet, VLAN, and home agent information for all mobility domains, or specify a mobility domain name to view data for that domain only.
global	View the current Mobility Agents global configuration

Parameter	Description
hat	Display the active Home Agent table
host	Display a list of Mobile IP hosts.
[<host-ip>]	Filter the Mobile Host List to display data for a specific host IPv4 address.
[<host-ipv6>]	Filter the Mobile Host List to display data for a specific host IPv6 address.
[<host-macaddr>]	Filter the Mobile Host List to display data for a specific host MAC address.
[brief]	Limit the output of this command to show just two lines of data.
multicast-vlan-table	Displays mobility multicast VLAN table information.
mac	MAC address of the client.
packet-trace [<count>]	The output of this command shows when packets of different types were sent between a source IP or MAC address and a destination IP or MAC address.
remote <host-ip> <host-ipv6> <host-macaddr>	This is a debug command can be used to identify the managed device associated with the specified client IPv4 or IPv6 address or MAC address. The output of this command shows the home agent (HA) and foreign agent (FA) for a mobile client, as well as the client's roaming status.
trace	Show if the Mobile IP feature will poll remote managed device for mobility status of station.
<host-ip>	Host IPv4 address.
<host-ipv6>	Host IPv6 address.
<mac-addr>	Host MAC address
force <host-ip> <host-ipv6> <mac-addr>	Show if the Mobile IP feature will poll remote managed device for mobility status of station.
traffic	Display mobile IP protocol statistics for: <ul style="list-style-type: none"> ■ Proxy Mobile IP ■ Home Agent Registrations ■ Foreign Agent Registrations ■ Registration Revocations
dropped	Show only counters for dropped mobility traffic.
foreign-agent	Show only mobile IP foreign agent statistics.

Parameter	Description
	A foreign agent is the managed device which handles all mobile IP communication with a home agent on behalf of a roaming client.
home-agent	Show only mobile IP home agent statistics. A home agent for a mobile client is the managed device where the client first appears when it joins the mobility domain.
proxy	Show only counters for mobile IP proxy traffic.
trail <host-ip> <host-ipv6> <host-macaddr>	Show the mobile IP roaming trail by entering a host's IP (IPv4 or IPv6) or MAC address.
tunnel	Show the Mobile Tunnel Table for IPIP tunnels.
visitor	Display a list of mobile nodes visiting a foreign agent.
[<host-ip>]	Filter the Foreign Agent Visitor list to display data for a specific host IPv4 address.
[<host-ipv6>]	Filter the Foreign Agent Visitor list to display data for a specific host IPv6 address.
[<host-macaddr>]	Filter the Foreign Agent Visitor list to display data for a specific host MAC address.
[brief]	Limit the output of this command to show just two lines of data.

Examples

The example below lists mobility domains configured on the managed device, and shows information for any subnets defined on these domains.

```
(host) [mynode] #show ip mobile domain

Mobility Domains:, 2 domain(s)
-----

Domain name default
  Home Agent Table, 0 subnet(s)

Domain name newdomain
  Home Agent Table, 2 subnet(s)
  subnet          mask          VlanId Home Agent      Description
  -----
-----
  10.2.124.76     255.255.255.255 1      10.4.62.2              Corporate
mobility entry
```

172.21.5.50 255.255.255.255 1 10.4.62.2 Reserved entries

The output of this command includes the following parameters:

Parameter	Description
Home Agent	IP address of the home agent or mobility agent.
Description	Description of the HAT entry.

Use the `show ip mobile host` command to track mobile users.

```
(host) [mynode] #show ip mobile host

Mobile Host List, 1 host(s)
-----
9c:b7:0d:3f:a6:dd 10.16.23.219  mob1
IPv4: 10.16.23.219
IPv6: fe80::826:aa9a:fe35:53e0
2004:deed::34
Roaming Status: Home Switch/Home VLAN, Service time 0 days 01:34:19
Home VLAN 623 on network 10.16.23.0/24
DHCP lease for PC at Sun Dec 23 20:32:00 2012 for 86400 secs from 10.16.28.1
```

The output of this command includes the following parameters:

Parameter	Description
<mac-addr> <ip-addr>	MAC and IP addresses of the host
Roaming Status	Displays how long the host has used its current managed device and VLAN.
Home VLAN	VLAN ID, IP address and subnet of the home VLAN.
DHCP lease	Displays the amount of time the station has had its current DHCP lease.

Related Commands

Command	Description
ip mobile active-domain	This command configures the mobility domain that is active on the managed device.

Command	Description
ip mobile domain	This command configures the mobility domain on the managed device.
ip mobile foreign-agent	This command configures the foreign agent for IP mobility.
ip mobile home-agent	This command configures the home agent for IP mobility.
ip mobile proxy	This command configures the proxy mobile IP module in a mobility-enabled managed device.
ip mobile revocation	This command configures the frequency at which registration revocation messages are sent.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip nat pool

```
show ip nat pool
```

Description

This command displays a pool of IP addresses for NAT.

Examples

The example below shows the current NAT pool configuration on Mobility Conductor.

```
(host) [mynode]# show ip nat pools

NAT Pools
-----
Name   Start IP      End IP         DNAT IP       Flags
----   -
2net   192.0.2.2     192.0.2.48    192.0.2.222
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the NAT pool.
Start IP	IP address that defines the beginning of the range of source NAT addresses in the pool.
End IP	IP address that defines the end of the range of source NAT addresses in the pool.
DNAT IP	Destination NAT IP address, if defined.
Flags	NAT pool flags, if any.

Related Commands

Command	Description
ip nat	This command configures a pool of IP addresses for NAT.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Enable or Config mode on Mobility Conductor.

show ip nexthop-list

```
show ip nexthop-list
  details STRING
  STRING
```

Description

This command displays the next hop list settings for policy-based routing. A next hop IP is the IP address of a adjacent router or device with layer-2 connectivity to managed device. The next hop list provides redundancy for the next hop devices by forwarding the traffic to a backup next hop device in case of failures. If active next hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next hop on the list. For more information on this feature, see [ip nexthop-list on page 871](#).

Parameter	Description
details	Displays detailed next hop settings for policy-based routing.
STRING	Displays the next hop settings based on the next hop list name.

Example

The following command displays the configuration settings for the one configured next hop list.

```
(host) [mynode] #show ip nexthop-list

Flags: N - Nexthop SLA non-compliant

Nexthop-List Entries
-----
Name          Dest  Preemptive Failover  Nexthop          Nexthop
Dest  Nexthop Priority  Wan Health-Check probe  SLA Profile
----  -
-----
load-balance-gateways          Enabled
load-balance-ipsecs           Enabled
pan-gp-ipsec-map-list         Enabled
test_nhl                       Enabled          145.145.145.10
  128                          Disabled
traditional-ipsecs            Enabled
```

The output of this command displays the following information

Parameter	Description
Name	Name of the next hop list
Dest	Destination prefix address.
Preemptive Failover	This column indicates whether preemptive failover is enabled or disabled. If preemption is enabled and a higher priority next hop becomes reachable again, packets are again forwarded to the higher priority next hop.
Nexthop	Next hop IP address.
Nexthop Dest	Next hop destination prefix address.
Nexthop Priority	List of the IP addresses of all next hop IPs, including the priority assigned to each device when the list was configured.
Wan Health-Check probe	Indicates weather the next hop failover is enabled or disabled.
SLA profile	Displays name of the IP-SLA profile configured to the next hop.

Related Commands

Command	Description
ip route	This command configures a static route on Mobility Conductor. (These routes can use a next hop list.)
ip nexthop-list	Configure next hop list settings for policy-based routing.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip ospf

```
show ip ospf
  database area <area-id>
  debug route
  ike-overlay aggregate-routes <addr>
  interface [tunnel|vlan] <id>
  neighbor
  rapng-vpn aggregate-routes <ip-addr> <mask>
  redistribute
  static aggregate-routes <addr>
  subnet
```

Description

Display statistics and configuration information for the OSPF routing protocol.

Parameter	Description
database area <area-id>	Show database information for the OSPF protocol.
debug route	Show debugging information for OSPF routes.
ike-overlay aggregate-routes <addr>	Show Ike overlay aggregate information for OSPF routes.
interface [tunnel vlan] <id>	Display the status of OSPF on an individual interface by specifying a tunnel or VLAN ID number. The tunnel ID range is 1-16777215.
neighbor	Display data for OSPF neighboring routers.
rapng-vpn	Display IAP-VPN information.
aggregate-routes <ip-addr> <mask>	Display IAP-VPN aggregate route information.
redistribute	Display OSPF route distribution information.
static aggregate-routes <addr>	Display STATIC Aggregate routes information.
subnet	Display the subnets manually added to the Subnet Exclude List via the router ospfsubnet exclude <addr> <mask> command.

Example

If you issue this command without any of the optional parameters described in the table above, the `show ip ospf` command will display general router and area settings for the OSPF.

```
(host) [mynode] #show ip ospf

OSPF is currently running with Router ID 123.45.110.200
Number of areas in this router is 1
Area 10.1.1.0
    Number of interfaces in this area is 2
    Area is totally stub area
    SPF algorithm executed 0 times
```

The output of this command includes the following parameters.

Parameter	Description
OSPF Router ID	Verifies that OSPF is running and the router ID that OSPF is running on.
Number of areas	List the number of areas configured in the router.
Area	Displays the Area ID followed by: <ul style="list-style-type: none"> ■ number of interfaces in the area ■ indicates if the area is a totally stub area ■ number of times the SPF algorithm has been executed

To display OSPF settings for an individual interface, you must specify a VLAN or tunnel ID number. The example below displays part of the output of the `show ip ospf interface vlan` command.

```
(host) [mynode] #show ip ospf interface vlan 1

Vlan 1 is up, line protocol is up
Internet Address 170.1.0.1, Mask 255.255.255.0, Area 2.0.1.1
Router ID 16.1.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 0
Designated Router id 0.0.0.0, Interface Address 170.1.0.1
Backup designated Router id 0.0.0.0, Interface Address 170.1.0.1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 7 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 7
Tx Err: BufNull 0 BufCorrupt 0 NoMem 0 SendFail 0
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
LoopSend 0 RxVirtualLink 0
Rx Err: DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
IntfDown 0 MySource 0 Legal 0
```

...

The output may include some or all of the following parameters.

Parameter	Description
Vlan <number>	Identifies that the interface type and ID are up and functional.
Internet Address	Internet address, network mask, and area assigned to the interface.
Router ID	Displays the router ID, that the network type is Broadcast, and the cost value.
Transmit Delay	Details of the transmit delay, state, and priority.
Designated Router	Details of the designated router ID and interface address.
Backup Designated Router ID	Details of the backup router ID and interface address.
Timer intervals configured	Details of elapse time intervals for Hello, Dead, Transmit (wait), and retransmit.
Neighbor Count	Details the number of neighbors and adjacent neighbors.
Tx Stat	Counters and statistics for transmitted data. <ul style="list-style-type: none"> ▪ Hellos: Number of transmitted hello packets. These packets are sent every hello interval. ▪ DbDescr: Number of transmitted database description packets. ▪ LsReq: Number of transmitted link state request packets. ▪ LsUpdate: Number of transmitted link state update packets. ▪ LsAck: Number of transmitted link state acknowledgment packets ▪ Pkts: Total number of transmitted packets.
Tx Err	Counters and statistics for received data. <ul style="list-style-type: none"> ▪ Hellos: Number of received hello packets. These packets are sent every hello interval. ▪ DbDescr: Number of received database description packets. ▪ LsReq: Number of received link state request packets. ▪ LsUpdate: Number of received link state update packets. ▪ LsAck: Number of received link state acknowledgment packets ▪ Pkts: Total number of received packets.
Rx Stat	Counters and statistics for received data. <ul style="list-style-type: none"> ▪ Hellos: Number of received hello packets. These packets are sent every hello interval. ▪ DbDescr: Number of received database description packets.

Parameter	Description
	<ul style="list-style-type: none"> ▪ LsReq: Number of received link state request packets. ▪ LsUpdate: Number of received link state update packets. ▪ LsAck: Number of received link state acknowledgment packets ▪ Pkts: Total number of received packets.
Rx Err	<p>Counters and statistics for received data.</p> <ul style="list-style-type: none"> ▪ Hellos: Number of received hello packets. These packets are sent every hello interval. ▪ DbDescr: Number of received database description packets. ▪ LsReq: Number of received link state request packets. ▪ LsUpdate: Number of received link state update packets. ▪ LsAck: Number of received link state acknowledgment packets ▪ Pkts: Total number of received packets.
DisCd	Number of received packets that are discarded.
BadVer	Number of received packets that have bad OSPF version number.
BadNet	Number of received packets that belong to different network than the local interface.
BadArea	Number of received packets that belong to different area than the local interface.
BadDstAdr	Number of received packets that have wrong destination address.
BadAuType	Number of received packets that have different authentication type than the local interface.
BadAuth	Number of received packets where authentication failed.
BadNeigh	Number of received packets which didn't have a valid neighbor.

Related Commands

Command	Description
interface vlan ip ospf	Configure OSPF on the interface.
router ospf	Configure OSPF on the router.

Command History

Release	Modification
ArubaOS 8.2.1.0	The <code>Tx Err</code> and <code>Rx Err</code> parameters were added to the output of the <code>show ip ospf interface vlan</code> command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip pppoe-info

```
show ip pppoe-info
```

Description

This command displays the configuration settings for PPPoE.

Examples

The following example displays the current PPPoE configuration.

```
(host) [mynode] #show ip pppoe-info

PPPoE username: rudolph123
PPPoE password: <HIDDEN>
PPPoE service name: ppp2056
PPPoE VLAN: 22
Gateway NAT: Enabled
IP: 10.1.1.1
PPPoE is UP
Server IP: 9.0.0.3
Gateway IP: 9.0.0.3
Primary DNS: <NONE> Secondary DNS: <NONE>
```

The output of this command includes the following parameters:

Parameter	Description
PPPoE username	PAP username configured on the PPPoE access concentrator.
PPPoE password	If this parameter displays the word <HIDDEN> , a PAP password is configured on the PPPoE access concentrator. If this parameter is <NONE> , there is no PPPoE password configured.
PPPoE service name	PPPoE service name.
PPPoE VLAN	VLAN configured to use PPPoE to obtain an IP address via the command <code>interface vlan <id> ip address pppoe</code> .

Related Commands

Command	Description
ap provisioning-profile	This command defines a provisioning profile for an AP or group of APs.

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the <code>show ip pppoe-info</code> command is modified to display Gateway NAT and IP parameters.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip probe

```
show ip probe
```

Description

This command displays the **health-check** profile settings for measuring WAN reachability and latency on a managed device uplink, and the **default** probe profile settings for PBR using next-hop lists.

The health-check feature uses ping or UDP probes for measuring WAN reachability and latency. PBR routing uses ping probes to determine the reachability of devices on a next-hop list. This command must be executed from the managed device only.

Examples

The following command displays the current IP probe settings for the **default** and **health-check** IP probe profiles.

```
(host-md) #show ip probe

IP Probe Entries
-----
Name           Probe Mode  Frequency(in sec)  Retries  Burst size
-----
default        Ping        10                 19       3
health-check   Ping        10                 3        5
```

The output of this command contains the following information:

Column	Description
Name	Name of the ip probe profile, which is either default or health-check .
Probe Mode	Indicates whether the probes are sent as ping or UDP packets.
Frequency	Probe interval, in seconds. The managed device sends the number of probes in the Burst Size column during each frequency interval.
Retries	Number of times the managed device attempts to resend a probe.
Burst size	Number of probes sent during the probe frequency interval that appears in the Frequency column.

Related Commands

Command	Description
ip probe default	This command configures IP probes for PBR using a next-hop list.
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ip radius

```
show ip radius
  nas-ip
  source-interface
```

Description

This command displays global parameters for configured RADIUS servers.

Parameter	Description
nas-ip	Show the Network Access Server (NAS) IP address attribute sent in outgoing RADIUS requests.
source-interface	Show the source interface address of outgoing RADIUS requests.

Examples

The following example displays the RADIUS client NAS IP address:

```
(host) [mynode] #show ip radius nas-ip
RADIUS client NAS IP address = 10.168.254.221
RADIUS client NAS IPv6 address = ::1
```

The following example displays the RADIUS client source interface address of the outgoing RADIUS requests:

```
(host) [mynode] #show ip radius source-interface
Global radius client source IP address = 12.0.2.26, vlan 3
Global radius client source IPv6 address = ::, vlan 0
Per-server client source IPv4/6 addresses:
```

Related Commands

Command	Description
ip radius	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip route

```
show ip route
  counters
  ike-overlay
  sdwan
  static
  stats
  verbose
```

Description

This command displays the Mobility Conductor routing table with static routes configured on the Mobility Conductor using the [ip route](#) command. Use the [ip default-gateway](#) command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Conductor.

Starting from ArubaOS 8.11.0.0, you can use the `ip default-gateway mgmt <nextthop>` command to configure the default gateway on the OOB management port for 7000 Series controllers.

Parameter	Description
counters	Displays the number of routes present, categorized by type.
ike-overlay	Displays ike-overlay routes.
sdwan	Displays sdwan routes.
static	Include this optional parameter to display only static routes.
stats	Displays route statistics.
verbose	Displays verbose information about routes.

Examples

The following example displays the IP address of routers and the VLANs to which they are connected:

```
(host) [mynode]#show ip route
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.7.73.77 to network 0.0.0.0 at cost 1
S*   0.0.0.0/0   [1/0] via 10.7.73.77*
S    172.0.0.0/8 [1/0] via 172.16.1.253*
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway for Mobility Conductor or the managed device.
ip route	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.11.0.0	The command output was modified to display the configured default gateway on the OOB management port for 7000 Series controllers.
ArubaOS 8.9.0.0	The command output was modified to display the configured default gateway on the OOB management port for 7280 controllers.
ArubaOS 8.2.1.0	The order of displaying the administrative distance and cost was changed to [AD/Cost] from [Cost/AD] in the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip tacacs

```
show ip tacacs
  source-interface
```

Description

This command displays global parameters for configured TACACS servers. The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
<code>source-interface</code>	Shows the source interface address of outgoing TACACS requests.

Examples

The following example displays the TACACS client source interface address of the outgoing TACACS requests:

```
(host) [mynode] #show ip tacacs source-interface
Global tacacs client source IP address = 0.0.0.0, vlan 0
Global tacacs client source IPv6 address = ::, vlan 0
Per-server client source IPv4/6 addresses:
```

Related Commands

Command	Description
ip radius	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip-flow-export

```
show ip-flow-export
  collector [<ipaddr>]
  gsm-cache
```

Description

This command shows information for IP flow collector and the GSM cache.

Parameter	Description
collector [<ipaddr>]	Specify the IP address of the collector.
gsm-cache	Shows GSM cache.

Example

The following command displays information about the IP flow collector.

```
(host) [mynode] #ip-flow-export collector

Observation Domain: 168096376 (Controller IP)
Collector IP Not Configured, protocol udp, port 4739, not enabled, not
connected
Upload template always, upload all sessions every 15 minute(s), no upload
flow cache snapshot
15000 flow cache size, 0 flows exported, next sequence 0, 0 packets, 0 bytes
Last template send: Never, last dispatch: Never
0 Connect errors, 0 connection resets, 0 send errors, 0 flows dropped, 0
blocked sends
(RJ_LC120) #show ip-flow-export collector 1.1.1.1
Observation Domain: 168096376 (Controller IP)
Collector IP 1.1.1.1, protocol udp, port 4739, not enabled, not connected
Upload template always, upload all sessions every 15 minute(s), no upload
flow cache snapshot
15000 flow cache size, 0 flows exported, next sequence 0, 0 packets, 0 bytes
Last template send: Never, last dispatch: Never
0 Connect errors, 0 connection resets, 0 send errors, 0 flows dropped, 0
blocked sends
No flows
```

Related Commands

Command	Description
ip dhcp pool	This command configures the IP flow collector profile. This command should be configured under /md.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip-flow-export wireless-cache

show ip-flow-export wireless-cache

Description

This command displays the cache for WLAN information.

Example

```
(host) [mynode] #show ip-flow-export wireless-cache

Flags: S - Source-ip, D - Dest-ip
IP Flow Export Wireless Cache
-----
STA ip      STA mac      ESSID                AP mac          Flags
-----
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  D
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  S
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  D
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  S
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  D
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  D
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  D
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  D
4.4.4.4     3c:77:e6:7c:47:9d  nbhardwaj-mm-psk     18:64:72:c7:33:1c  S
6.6.6.4     5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk  9c:1c:12:c0:86:9c  S
```

Related Commands

Command	Description
ip-flow-export-profile	This command configures the IP flow collector profile.

Command History

Version	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config or Enable mode on Mobility Conductor.

show ip-flow-export-profile

show ip-flow-export-profile

Description

This command shows the stats for IP flow collector profile.

Example

The following command displays details for the IP flow export profile

```
(host) [mynode] #show ip-flow-export-profile

IP Flow Collector Profile
-----
Parameter                               Value      Set
-----
State                                    Disabled
Interval (minutes) to upload all active sessions 15
Interval (minutes) to upload cache snapshot      0
Interval (minutes) to upload IPFIX template     0
Transport Protocol for collector connection     udp
IPFIX Collector IP address                     N/A
Transport Port for collector connection        4739
Flow Cache size in entries                     15000
Observation Domain                            0
```

Related Commands

Command	Description
ip-flow-export-profile	This command configures the IP flow collector profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipc statistics

```
show ipc statistics
  app-ap
  app-id
  app-name
```

Description

This command displays the Inter Process Communication (IPC) statistics.

Parameter	Description
app-ap	Displays the Inter Process Communication (IPC) statistics for a specific AP or BSSID.
app-id	Application ID number. This number must be obtained from Aruba TAC.
app-name	Displays Inter Process Communication (IPC) statistics for a specific application.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor or Managed Device.

show ipc statistics app-ap

```
show ipc statistics app-ap {am|ap-stm|ofald|sapd}
  ap-name <ap-name>
  bssid <bssid>
  ip-addr <ip-addr>
```

Description

This command displays the Inter Process Communication (IPC) statistics for a specific AP or BSSID. Execute this command under the supervision of Aruba TAC to troubleshoot application errors. This command must be executed on a standby controller or managed device where the APs terminate.

Parameter	Description
am	Show IPC statistics for an air monitor.
ap-stm	Show IPC statistics for AP station management communication.
ofald	OpenFlow Agent Lite Daemon. Show OpenFlow Agent statistics running on the AP.
sapd	Show IPC statistics for the AP management process on the AP.
ap-name <ap-name>	Show IPC statistics for an AP with a specific name.
bssid <bssid>	Show IPC statistics for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
ip-addr <ip-addr>	Show IPC statistics for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Example

The following example shows IPC statistics for the station management process on an AP named **corp-AP-115**.

```
(host-md) #show ipc statistics app-ap ap-stm ap-name corp-AP-115
IP: 168778491, IP_STR: 10.15.90.251

Local Statistics
To application      Tx Msg   Tx Blk   Tx Ret   Tx Fail   Rx Ack   Rx Msg   Rx
Drop  Rx Err  Tx Ack   Rx Silent Drops
SAPM Client
  0      0      0      0      0      0      40
```



```

Kernel PAPI Statistics
RxSockbufSize RxSockbufHimark CurRxQLen MaxRxQLen Drops
0 0 0 0 0
Remote Device 10.15.88.100 Statistics
To application Tx Msg Tx Blk Tx Ret Tx Fail Rx Ack Rx Msg Rx
Drop Rx Err Tx Ack Rx Silent Drops
14302 0 0 1 0 0 0 0 0 1
0 0 1 0
Allocated Buffers 1
Static Buffers 4
Static Buffer Size 1400

```

The output of this command includes the following data columns:

Parameter	Description
Tx Msg	Number of transmitted messages.
Tx Blk	Number of blocking messages transmitted.
Tx Ret	Number of transmitted messages that were returned.
Tx Fail	Number of failure messages that were transmitted.
Rx Ack	Number of received acknowledgments.
Rx Msg	Number of received messages.
Rx Drop	Number of received messages that were dropped.
Rx Err	Number of received messages with errors.
Tx Ack	Number of transmitted acknowledgments.
Allocated Buffers	Number of allocated buffers for IPC messages.
Static Buffers	Number of static buffers for IPC messages.
Static Buffer Size	Size of the static buffer.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ipc statistics app-id

```
show ipc statistics app-id <app-id>
```

Description

This command displays the Inter Process Communication (IPC) statistics for a specific AP or BSSID. Execute this command under the supervision of Aruba TAC to troubleshoot application errors.

Parameter	Description
<app-id>	Application ID number. This number must be obtained from Aruba TAC.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor or Managed Device.

show ipc statistics app-name

show ipc statistics app-name <name>

Description

Display Inter Process Communication (IPC) statistics for a specific application. Execute this command under the supervision of Aruba TAC to troubleshoot application errors.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<name>	One of the following application names: <ul style="list-style-type: none">▪ aaa: Administrator Authentication▪ ads: Anomaly Detection▪ auth-resp: Authentication Response▪ authmgr: User Authentication▪ certmgr: Certificate Manager▪ cfgm: Config Manager▪ cluster_mgr: Cluster Manager▪ cpsec: Control-Plane Security Manager▪ cts: Transport Service▪ dbsync: Database Synchronization▪ dds: Distributed data store▪ dhcp: DHCP Server▪ esi: Server Load Balancing▪ extifmgr: External Interface Manager▪ fpapps: Layer 2,3 control▪ gsmmgr: GSM manager▪ ha_mgr: HA manager▪ httpd: HTTPD▪ ike: IKE Daemon▪ l2tp: L2TP▪ lagm: LAGM▪ licensemgr: License Manager▪ mdns: AirGroup mdns▪ mobileip: Mobile IP▪ ntp: NTP Daemon▪ ofa: OpenFlow Agent▪ ospf: OSPF▪ phonehome: PhoneHome▪ pim: Protocol Independent Multicast▪ pktfilter: Packet Filter


```

RxSockbufSize RxSockbufHimark CurRxQLen MaxRxQLen Drops
16777216          1152          0          1          0
Remote Device 10.4.176.95 Statistics
To application      Tx Msg   Tx Blk   Tx Ret   Tx Fail   Rx Ack   Rx Msg
SAPM                2565     0         0         0         0       2667
Rx Drop   Rx Err   Tx Ack   Tx Sign Rx Sign Rx Denied Rx Silent Drops
    0         0         0         0       0       0         0

Remote Device 172.200.13.3 Statistics
To application      Tx Msg   Tx Blk   Tx Ret   Tx Fail   Rx Ack   Rx Msg
SAPM                2569     0         0         0         0       2569
Rx Drop   Rx Err   Tx Ack   Tx Sign Rx Sign Rx Denied Rx Silent Drops
    0         0         0         0       0       0         0
Allocated Buffers   4
Static Buffers      0
Static Buffer Size  1476

```

The output of this command includes the following data columns:

Parameter	Description
Tx Msg	Number of transmitted messages.
Tx Blk	Number of blocking messages transmitted.
Tx Ret	Number of transmitted messages that were returned.
Tx Fail	Number of failure messages that were transmitted.
Rx Ack	Number of received acknowledgments.
Rx Msg	Number of received messages.
Rx Drop	Number of received messages that were dropped.
Rx Err	Number of received messages with errors.
Tx Ack	Number of transmitted acknowledgments.
Tx Sign	Number of messages which were signed before transmitting.
Rx Sign	Number of messages validated through digest validation.
Rx Denied	Number of messages denied due to incorrect digest.
Rx Silent Drops	Number of received messages that are categorized as silent drops.
Allocated Buffers	Number of allocated buffers for IPC messages.

Parameter	Description
Static Buffers	Number of static buffers for IPC messages.
Static Buffer Size	Size of the static buffer.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>lagm</code> and <code>vrp</code> parameters were added.
ArubaOS 8.0.1.0	Tx Sign , Rx Sign , and Rx Denied columns are added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor or Managed Device.

show ipstm

show ipstm debug stats

Description

This command displays the debug messages for the IPsec tunnel manager.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv4 user-table

```
show ipv4 user-table
  ap-group <ap-group>
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  ap-name <ap-name>
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  authentication-method {dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web}
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  bssid <A:B:C:D:E:F>
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  debug
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  essid <STRING>
    ip
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  internal
    rows <start-row> <no-of-rows>
  ip <addr> [log]
  mac <A:B:C:D:E:F>
  mobile
    bindings [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
    rows <start-row> <no-of-rows>
    unique
      bindings [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
      rows <start-row> <no-of-rows>
      visitors [rows <start-row> <no-of-rows>]
      visitors [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
  name <STRING> [unique]
  phy-type {[a]|[b]}
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  role <STRING>
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
  rows <start-row> <no-of-rows>
  station
  verbose
    rows <start-row> <no-of-rows>
    unique [rows <start-row> <no-of-rows>]
```

Description

This command displays the IPv4 user table entries. You can filter the output based on various parameters described in the following table. This command should be executed from the managed device only where the APs and client terminate.

Parameter	Description
ap-group <ap-group>	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
ap-name <ap-name>	Filter the output of this command by showing users connected to an AP with the specified AP name.
authentication-method	Filter the output of this command by the authentication method used for the device:
dot1x	Filter the output of this command by showing data for devices using the 802.1X authentication.
mac	Filter the output of this command by showing data for devices using the MAC authentication.
opensystem	Filter the output of this command by showing data for devices using the open (no) authentication.
psk	Filter the output of this command by showing data for devices that do not use authentication but use a PSK for encryption.
stateful-dot1x	Filter the output of this command by showing data for devices using stateful 802.1X authentication.
via-vpn	Filter the output of this command by showing data for devices that authenticate using VIA.
vpn	Filter the output of this command by showing data for devices using VPN authentication.
web	Filter the output of this command by showing data for devices using the Captive Portal authentication.
bssid	Filter the output of this command by showing users connected to the specified BSSID.
debug	Filter the output of this command by showing entries in the IPv4 user-table that are in debug mode.
ssid	Filter the output of this command by showing entries in the IPv4 user table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Filter the output of this command by showing internal IPv4 users.
ip <A.B.C.D>	Filter the output of this command by showing IPv4 users that match the specified IPv4 address.
log	Filter the output of this command by showing the log information for the specified IPv4 client.

Parameter	Description
mac	Filter the output of this command by showing users with the specified MAC address.
mobile	Filter the output of this command by showing a list of mobile users in the IPv4 user table. The following filters are available for this parameter: <ul style="list-style-type: none"> ▪ bindings—List of users that have moved away from the current managed device. ▪ rows—Displays entries that match the specified row number. ▪ unique—Displays unique entries in the IPv6 user-table. ▪ visitors—Displays users that have associated with the current managed device.
name	Filter the output of this command by showing IPv4 user table entries that match the specified name.
phy-type	Filter the output of this command by showing IPv4 user table entries that match a or b phy-type.
role	Filter the output of this command by showing IPv4 user table entries that match the specified role.
rows	Filter the output of this command by showing specific rows in the IPv4 user table. Enter the starting row number and the number of rows to be displayed.
station	Filter the output of this command by showing the station table information for the IPv4 user table entries.
verbose	Filter the output of this command by showing the complete IPv4 user table with all details.

Example

The following example displays a list of internal IPv4 user entries:

```
(host-md) #show ipv4 user-table
IP                MAC                Name      Role                Age (d:h:m)
Auth
-----
192.168.201.234   00:10:18:a9:38:e1   uccsol10  ucc-dot1x-voice    00:22:14
802.1X
192.168.201.230   5c:c5:d4:7d:c0:80   uccsol23  ucc-dot1x-voice    00:02:59
802.1X
192.168.201.252   48:51:b7:19:40:88   uccsol19  ucc-dot1x-voice    00:22:14
802.1X
```

```

192.168.201.241 5c:c5:d4:7d:c2:b5 uccsol24 ucc-dot1x-voice 00:02:59
802.1X
192.168.201.233 5c:c5:d4:7d:c0:b7 uccsol22 ucc-dot1x-voice 00:02:29
802.1X

VPN link  AP name  Roaming  Essid/Bssid/Phy  Profile
Forward mode
-----  -
-----

          115-1    Wireless UCC-DOT1X/ac:a3:1e:27:e4:b1/a-HT  UCC-DOT1X dtunnel
          325-1    Wireless UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X dtunnel
          325-1    Wireless UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X dtunnel
          325-1    Wireless UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X dtunnel
          325-1    Wireless UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X dtunnel

Type  Host Name
----  -
User Entries: 5/5

```

The output of this command includes the following parameters:

Output	Description
IP	IP address of the client in that row that authenticating using 802.1X authentication.
MAC	MAC address of the client.
Name	Name of the client.
Role	The role assigned to the client.
Age (d:h:m)	Total time that client is connected to managed device.
Auth	Authentication type of the client.
VPN link	Clients using VPN authentication.
AP name	Name of the AP associated with the client.
Roaming	Current roaming status of the client.
Essid/Bssid/Phy	ESSID, BSSID, and Phy to which the client is associated.
Profile	The AAA profile to which the client is associated.
Forward Mode	The client traffic forwarding mode.

Related Commands

Command	Description
show user-table	Displays detailed information about the controller's connection to a user device, in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ipv6

```
show ipv6
  dhcp
  dhcp-client
  firewall
  global
  interface
  mld
  neighbors
  netlink
  nexthop-list
  pd
  ra
  route
  user-table
```

Description

Shows IPv6 commands.

Parameter	Description
dhcp	Show DHCPv6 information.
dhcp-client	Shows DHCPv6 client lease information.
firewall	Shows IPv6 firewall configuration.
global	Provides IPv6 global config information.
interface	Shows IPv6 interface information.
mld	Shows MLD information.
neighbors	Show IPv6 neighbor cache entries.
netlink	Show netlink information.
nexthop-list	Shows IPv6 Nexthop-lists configured on this controller.
pd	Shows IPv6 Prefix Delegation.
ra	Shows IPv6 Router Advertisements.
route	Shows IPv6 Routing table.
user-table	Shows internal user table.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 dhcp

```
show ipv6 dhcp
  binding
  database {pool <pool_name>}
  helper <id>
  relay <counters>
  relay-option
  vlan <id>
```

Description

This command displays the DHCPv6 server settings.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
binding	Show DHCPv6 server bindings.
database [pool<pool_name>]	Show DHCPv6 server settings.
helper <id>	Show DHCPv6 helper information.
relay <counters>	Show DHCPv6 relay information.
relay-option	Show DHCPv6 relay option configurations.
vlan <id>	Show DHCPv6 VLAN information. <1-4094> VLAN ID

Examples

The following example shows the DHCPv6 database:

```
(host) [mynode] #show ipv6 dhcp database
DHCPv6 enabled
# 2001-feed-64-nw
subnet6 2001:feed::/120 {
    option vendor-class-identifier "ArubaAP";
    option dhcp6.vendor-opts "2001:feed::235";
    range6 2001:feed::1 2001:feed::234;
    range6 2001:feed::236 2001:feed::ffff:ffff:ffff:fffe;
}
# 2003-feed-64-nw
subnet6 2003:feed::/120 {
```



```

    option vendor-class-identifier "ArubaAP";
    option dhcp6.vendor-opts "2001:feed::235";
    range6 2003:feed::1 2003:feed::234;
    range6 2003:feed::236 2003:feed::ffff:ffff:ffff:fffe;
}
# DHCPv6
subnet6 2001:470:faca:4::/120 {
    default-lease-time 43200;
    max-lease-time 43200;
    option dhcp6.domain-search "test.org";
    option vendor-class-identifier "ArubaAP";
    option dhcp6.vendor-opts "2001:feed::235";
    option dhcp6.name-servers 2001:470:20::2;
    option dhcp6.preference 25;
    option dhcp6.usr-opt-24-DHCPv6 "Domain Search List";
    range6 2001:470:20::1 2001:470:faca:4::1;
    range6 2001:470:20::3 2001:470:faca:4:ffff:ffff:ffff:fffe;
}

```

The following example shows the DHCPv6 database for a specific pool:

```

(host) [mynode] #show ipv6 dhcp database [pool <pool-name>]
(host) [mynode] #show ipv6 dhcp database pool DHCPv6

# DHCPv6
subnet6 2001:470:faca:4::/120 {
    default-lease-time 43200;
    max-lease-time 43200;
    option dhcp6.domain-search "test.org";
    option vendor-class-identifier "ArubaAP";
    option dhcp6.vendor-opts "2001:feed::235";
    option dhcp6.name-servers 2001:470:20::2;
    option dhcp6.preference 25;
    option dhcp6.usr-opt-24-DHCPv6 "Domain Search List";
    range6 2001:470:20::1 2001:470:faca:4::1;
    range6 2001:470:20::3 2001:470:faca:4:ffff:ffff:ffff:fffe;
}

```

The following example shows the DHCPv6 binding information:

```

(host) [mynode] # show ipv6 dhcp binding
# Client: fe80::1cf:2e1:cd13:356b; IA ID 0x13001f3c
ia-na "\023\000\037<\000\001\000\001\030\223\211\242\000%\263J\372\364" {
    cltt epoch 1364206514; # Mon Mar 25 15:45:14 2013
    iaaddr 2001:470:faca:4:21a:1eff:fe00:9e6 {
        binding state expired;
        preferred-life 187;
        max-life 300;
        ends epoch 1364206814; # Mon Mar 25 15:50:14 2013
    }
}

```

The following example shows the DHCPv6 active pools:

```
(host) [mynode] #show ipv6 dhcp active-pools
DHCPv6 Active Pools
-----
Vlan Pool Name
-----
10   DHCPv6
```

The following example shows the DHCPv6 VLAN information:

```
(host) [mynode] (config) #show ipv6 dhcp vlan 1

DHCPv6 Vlan 1 Table
-----
VLAN  PREFIX                HELPER ADDRESS    RELAY OPTION
----  -
1     2002::1, 2004::2         2444::2, 2333::2 L3-Enabled
```

The following example shows the DHCPv6 helper information:

```
(host) #show ipv6 dhcp helper
DHCPv6 User Table
-----
VLAN  HELPER ADDRESS  SOURCE ADDRESS
----  -
3     2444::2         2002::1
3     2333::2         2004::2
```

The following example shows the DHCPv6 relay-option information:

```
(host) #show ipv6 dhcp relay-option
DHCPv6 relay option XML File: test.xml
Circuit-Id:<Client MAC in lower-case with ':' as delimiter>
Remote-Id:<Client MAC in lower-case with ':' as delimiter>
```

Related Commands

Command	Description
ipv6 dhcp pool	This command configures a DHCPv6 pool on the managed device.

Command History

Release	Modification
ArubaOS 8.8.0.0	The following parameters were introduced: <ul style="list-style-type: none"> ■ helper <id> ■ relay <counters> ■ relay-option ■ vlan <id>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 dhcp-client

show ipv6 dhcp-client

Description

Shows DHCPv6 client lease information.

Examples

The example below shows the DHCPv6 database:

```
(host) [mynode] #show ipv6 dhcp-client
DHCPv6 enabled
# 2001-feed-64-nw
subnet6 2001:feed::/120 {
    option vendor-class-identifier "ArubaAP";
    option dhcp6.vendor-opts "2001:feed::235";
    range6 2001:feed::1 2001:feed::234;
    range6 2001:feed::236 2001:feed::ffff:ffff:ffff:fffe;
}
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 firewall

```
show ipv6 firewall
```

Example

This example displays the status of all firewall configurations.

```
(host) [mynode] #show ipv6 firewall
Global IPv6 firewall policies
-----
Policy                               Action   Rate   Port
-----
Monitor TCP SYN attack                Disabled
Monitor IPv6 sessions attack          Disabled
Deny inter user bridging              Disabled
Drop all IPv6 fragments                Disabled
Per-packet logging                    Disabled
Enforce TCP handshake before allowing data Disabled
Prohibit RST replay attack             Disabled
Session Idle Timeout                  Disabled
Prohibit IPv6 Spoofing                 Disabled
Extension header parse length          Disabled
Stateful ICMP Processing                Disabled
Enforce TCP Sequence numbers           Disabled
```

The output of this command includes the following parameters:

Output	Description
Monitor TCP SYN attack	If enabled, the managed device monitors the number of TCP SYN messages per second. If this value exceeds the maximum configured rate, the managed device will register a DoS attack.
Monitor IPv6 sessions attack	If enabled, the managed device monitors the number of TCP session requests per second. If this value exceeds the maximum configured rate, the managed device will register a DoS attack sessions.
Deny inter user bridging	If enabled this setting prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.

Output	Description
Drop all IPv6 fragments	If enabled, all IPv6 fragments are dropped.
Per-packet logging	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.
Enforce TCP handshake before allowing data	If enabled, this feature prevents data from passing between two clients until the three-way TCP handshake has been performed. Enabling this option causes mobility to fail. So, disable this option if you have mobile clients on the network as.
Prohibit RST replay attack	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.
Session Idle Timeout	Shows if a session idle timeout interval has been defined.
Prohibit IPv6 Spoofing	Status on IPv6 spoofing. When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
Extension header parse length	Shows the extension header parse length, with a maximum value of 100 bytes.
Stateful ICMP Processing	If enabled, stateful ICMP processing is enabled.
Enforce TCP Sequence numbers	
Enable session-spread	

Related Commands

Command	Description
ipv6 firewall	This command configures firewall options on the Mobility Conductor for IPv6 traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 global

```
show ipv6 global
```

Description

Displays IPv6 global config information.

Example

The following example displays the global status of the IPv6 packet.

```
(host) [mynode] #show ipv6 global
Global IPv6 Packet Processing is Enabled
```

Related Commands

Command	Description
ipv6 enable	This command enables IPv6 packet processing globally. This option is disabled by default.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 interface

show ipv6 interface [brief]

Description

View ipv6 related information on all interfaces.

Parameter	Description
brief	Optional parameter. If specified, displays the ipv6-related information on all the interfaces in a summary format.

Example

```
(host) [mynode] #show ipv6 interface
VLAN1 is up line protocol is down
IPv6 Router Advertisements are disabled
IPv6 is disabled
VLAN46 is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e00:2e00:9f0
Global unicast address(es):
2046:eab::25, subnet is 2046:eab::/64
IPv6 Router Advertisements are disabled
VLAN50 is up line protocol is up
IPv6 Router Advertisements are disabled
IPv6 is disabled
VLAN10 is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e00:a00:9f0
Global unicast address(es):
2010:eab::1, subnet is 2010:eab::/64
fc01:eab::1, subnet is fc01:eab::/64
IPv6 Router Advertisements are enabled
loopback is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e0f:ff00:9f0
Global unicast address:
2046:eab::2, subnet is 2046:eab::2/128
TUNNEL2 is up line protocol is up
tunnel mode is Layer2 IPv6 GRE, tunnel vlan 10
tunnel source ipv6 address is 2046:eab::25
tunnel destination ipv6 address is 2047:eab::25

(host) [mynode] #show ipv6 interface brief
Interface                [Status/Protocol]
vlan 800                  [ up/up ]
    unassigned
vlan 1                    [ up/down]
    unassigned
vlan 802                  [ up/up ]
    fe80::b:8603:226d:863c/64
```

```

2082::802:1/64
vlan 32                [ up/up ]
  unassigned
vlan 801               [ up/up ]
  fe80::b:8603:216d:863c/64
  2005:81::1/64
vlan 50                [ up/down]
  fe80::b:8600:326d:863c/64
  2050:3::50:1/64
loopback               [ up/up ]
  fe80::b:860f:ff6d:863c/64
mgmt                   [down/down]
  unassigned
tunnel 2               [ up/up ]
  unassigned

```

The following table details the columns and content in the show command.

Column	Description
Interface	List the interface and interface identification with the IPv6 address and netmask for the interface, if configured.
Status/Protocol	States the administrative status and the IPv6 status on the interface. <ul style="list-style-type: none"> ▪ Enabled—up ▪ Disabled—down

Related Commands

Command	Description
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 mld

```
show ipv6 mld
  cluster
  config
  counters
  group
  interface
  proxy-group
  proxy-mobility-group
  proxy-mobility-stats
  proxy-stats
```

Description

Shows MLD information.

Parameter	Description
cluster	Shows cluster information.
config	Shows MLD configuration.
counters	Shows MLD counters.
group	Shows MLD group information.
interface	Shows MLD interface information.
proxy-group	Shows interface specific MLD proxy group information.
proxy mobility group	Shows interface specific MLD proxy mobility group information.
proxy-mobility-stats	Shows MLD proxy mobility specific statistics.
proxy-stats	Shows MLD proxy specific statistics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld cluster

```
show ipv6 mld cluster
  aac-info
  bss-info
  client-info
  dmo-off-info
  info
  proxy-group
  stats
```

Description

Display MLD configuration details for a cluster.

Parameter	Description
aac-info	Show cluster AAC information of APs.
bss-info	Show IGMP BSS information.
client-info	Show IGMP cluster client information.
dmo-off-info	Show list of (S,G,BSS) where DMO threshold is hit.
info	Show cluster information.
proxy-group	Show IGMP cluster proxy database group information.
stats	Show cluster statistics.

Example

The following example displays output of the `show ipv6 mld cluster` command.

```
(host)[node] # show ipv6 mld cluster
Cluster information

Clustering      Enabled
Version        IPv6
Redundancy     Enabled

TABLE
-----
Controller IP      Connected State  Multicast Vlan  Priority
-----
Self              Yes              0                128
2002:192:168:211::2  Yes              0                128
```

Related Commands

Command	Description
ipv6 mld	This command configures the IPv6 MLD (Multi-listener discovery) parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on managed device.

show ipv6 mld config

```
show ipv6 mld config
```

Description

Displays MLD configuration details.

Example

This example displays the current MLD configuration values.

```
(host) [mynode] #show ipv6 mld config
MLD Config
-----
Name                Value
-----
robustness-variable 2
query-interval      125
query-response-interval 100
max-members-per-group 300
ssm-range           FF3X::4000:1 - FF3X::FFFF:FFFF
```

The output of this command includes the following parameters:

Output	Description
robustness-variable	Denotes the value that is used to calculate the timeout value of an MLD client.
query-interval	Denotes the time interval at which the MLD query is sent.
query-response-interval	Denotes the time interval at which the MLD query response should be received.
max-members-per-group	Denotes the maximum members per group.
ssm-range	Denotes the source specific multicast range. When you enter the SSM Range ensure that the upstream router has the same range, else the multicast stream would be dropped. NOTE: Only SSM enabled clients can subscribe to the multicast stream in the multicast range. The default ssm-range in case of IPv6 is FF3X::4000:1 - FF3X::FFFF:FFFF, this range is configurable. If MLDv1 or a non SSM client sends a report on a specified SSM range, it is rejected by the managed device.

Related Commands

Command	Description
ipv6 mld	This command configures the IPv6 MLD (Multi-listener discovery) parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld counters

show ipv6 mld counters

Description

Displays the statistics of MLD.

Example

This example displays the MLD statistics for the following values.

```
(host) [mynode] #show ipv6 mld counters
MLD Statistics
-----
Name                Value
----                -
received-total      0
received-queries    0
received-v1-reports 0
received-v1-leaves  0
received-v2-reports 0
received-unknown-types 0
len-errors           0
checksum-errors     0
not-vlan-dr         0
transmitted-queries 0
forwarded            0
non-conforming-mld  0
```

The output of this command includes the following parameters:

Output	Description
received-total	The total number of MLD messages.
received-queries	The total number of MLD queries.
received-v1-reports	The total number of MLD v1 reports received.
received-v1-leaves	The total number of MLD v1 leave messages received.
received-v2-reports	The total number of MLD v2 reports received.
received-unknown-types	The total number of unrecognized messages received.
len-errors	The total number of error message where the length check has failed.

Output	Description
checksum-errors	The total number of error message where the checksum has failed.
not-vlan-dr	The number of messages received for which the current managed device is not the designated router.
transmitted-queries	The total number of transmitted MLD queries.
forwarded	The total number of MLD messages forwarded.
non-conforming-mlد	The total number of non confirming MLD messages.

Related Commands

Command	Description
ipv6 mld	This command configures the IPv6 MLD (Multi-listener discovery) parameters.
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld group

show ipv6 mld group

Example

This example displays MLD group details.

```
(host) [mynode] #show ipv6 mld group
MLD Group Table
-----
Group                Members  Mode    Age
-----
ff02::1:ff00:0       2        Exclude  4
ff02::1:ff00:1900    2        Exclude  1
ff1e::2              2        Include  0
ff02::1:3            4        Exclude  1
ff02::202            2        Exclude  4
ff02::2              3        Exclude  1
ff02::1:ff20:d6e2    2        Exclude  4
ff02::c              4        Exclude  2
ff02::1:ffab:4027    2        Exclude  6
ff02::d              2        Exclude  1
ff02::1:ff00:12      2        Exclude  4
ff02::1:ffd6:4d41    1        Exclude  7
ff02::16             2        Exclude  1
ff02::1:ffd6:4d40    1        Exclude  1
ff02::1:ff8a:4951    2        Exclude  4
ff02::1:ff5b:aac4    2        Exclude  11
ff02::1:ff9f:df01    2        Exclude  3
Total Groups: 17
```

The output of this command includes the following parameters:

Output	Description
Group	Name of MLD groups.
Members	Number of members in an MLD group.
Mode	Managed device supports two IPv6 multicast source filtering modes - Include and Exclude. In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses (MLDv1 mode).
Age	This parameter specifies the aging time.

This example displays MLD group address details.

```
(host) [mynode] #show ipv6 mld group maddr ff1e::2 mac 9c:b7:0d:3f:a8:fc
MLD member 9c:b7:0d:3f:a8:fc Table
-----
Source          Age
-----
2001:feed::2   26
```

The output of the `show ipv6 mld group` command includes the following parameters:

Parameter	Description
Source	IP address of the multicast source.
Age	This parameter specifies the aging time.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld interface

```
show ipv6 mld interface
```

Example

This example displays MLD status on VLANs. To view details for a specific VLAN, you can specify the VLAN ID.

```
(host) [mynode] #show ipv6 mld interface
MLD Interface Table
-----
VLAN  Link local address  Snooping  Proxy    Querier  Querier-dest
Upstream querier  Upstream port
-----
-----
1      ::                    disabled  disabled  ::       unknown   ::
      -
160    ::                    disabled  disabled  ::       unknown   ::
      -
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	Denotes the VLAN ID.
Link local address	IP address of the VLAN interface.
Snooping	Status of MLD snooping.
Proxy	Status of MLD proxy configuration.
Querier	IPv6 address of the MLD querier for the VLAN.
Querier-dest	Denotes the destination of MLD querier on VLAN.
Upstream querier	Denotes the address of upstream MLD querier on VLAN.
Upstream port	Denotes the destination of upstream MLD querier on VLAN.

Related Commands

Command	Description
ipv6 mld	This command configures the IPv6 MLD (Multi-listener discovery) parameters.
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld proxy-group

```
show ipv6 mld proxy-group [vlan <vlan>]
```

Example

This example displays MLD proxy-group details.

```
(host) [mynode] #show ipv6 mld proxy-group
MLD Proxy Group Table
-----
VLAN  Addr                Group                Num Members
----  -
10    fe80::b:8600:a61:cc5c  ff1e::5             2
10    fe80::b:8600:a61:cc5c  ff02::1:ff9e:dc4c  1
10    fe80::b:8600:a61:cc5c  ff02::1:3           2
10    fe80::b:8600:a61:cc5c  ff02::1:ff83:d718  1
10    fe80::b:8600:a61:cc5c  ff02::1:ff13:356b  1
10    fe80::b:8600:a61:cc5c  ff02::c             2
Total displayed proxy groups: 6
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	Denotes the VLAN ID.
Addr	IP address of the VLAN interface.
Group	Name of MLD group.
Num Members	Number of members in an MLD group.

Related Commands

Command	Description
ipv6 mld	This command configures the IPv6 MLD (Multi-listener discovery) parameters.
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld proxy-mobility-group

```
show ipv6 mld proxy-mobility-group [maddr <maddr>]
```

Example

This example displays MLD proxy-mobility-group details.

```
(host) [mynode] #show ipv6 mld proxy-mobility-group
MLD MIP Group Table
-----
Group      Members
-----
ff1e::2    1
ff02::1:3  2
ff02::c    1
```

The output of this command includes the following parameters:

Parameter	Description
Group	Name of MLD mobility group.
Members	Number of members in an MLD mobility group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld proxy-mobility-stats

```
show ipv6 mld proxy-mobility-stats
```

Example

This example displays the details of MLD proxy-mobility statistics.

```
(host) [mynode] #show ipv6 mld proxy-mobility-stats
MLD Mobility Multicast Statistics
-----
Name                Sent  Received
----                -    -
Joins                -    2
Leaves               -    0
Intra-move           -    1
Inter-move           -    0
Client-away          -    0
Back-home            -    0
Query-db             -    0
Query-foreign-db    -    0
Query-home-db        -    0
Add-visitor          -    0
Replies              0    -
```

The output of this command includes the following parameters:

Parameter	Description
Name	Type of packet.
Sent	Number of packets sent.
Received	Number of packets received.

Related Commands

Command	Description
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 mld proxy-stats

```
show ipv6 mld proxy-stats
```

Example

This example displays the status of the MLD proxy.

```
(host) [mynode] #show ipv6 mld proxy-stats
MLD Proxy Statistics (Upstream)
-----
Name      Sent   Received
-----
Queries  -     39
Joins    51    112
Leaves   9      0
```

The output of this command includes the following parameters:

Parameter	Description
Name	Type of packet.
Sent	Number of packets sent.
Received	Number of packets received.

Related Commands

Command	Description
interface vlan	This command configures a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 neighbors

```
show ipv6 neighbors
  counters
  vlan
```

Description

Displays the IPv6 neighbors configured on a VLAN interface. This command displays the IPv6 neighbors configured on a VLAN interface via the [ipv6 neighbor](#) command.

Description

Shows IPv6 commands.

Parameter	Description
counters	Shows neighbor cache counters.
vlan	Shows the vlan Ids.

Examples

The example below shows the ipv6 neighbors configured on VLAN 1 .

```
(host) [mynode] #show ipv6 neighbors vlan 1
IPv6 Neighbors
-----
IPv6 Address          Age   Link-layer Addr      State      Interface
-----
2cce:205:160:100::fe  -    00:0b:86:61:13:28    PERMANENT  vlan 1
```

Related Commands

Command	Description
ipv6 neighbor	This command configures an IPv6 static neighbor on a VLAN interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 netlink

```
show ipv6 netlink
  stats
```

Description

This command displays the netlink information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
stats	Displays netlink statistics.

Examples

The following example shows the netlink statistics:

```
(host) [mynode] #show ipv6 netlink stats

IPv6 address add total           : 3
IPv6 address add DAD fail       : 0
IPv6 address delete total      : 2
IPv6 link up total              : 0
IPv6 link down total            : 0
IPv6 add route total            : 13
IPv6 add route destination      : 12
IPv6 add route source           : 0
IPv6 add route gateway          : 0
IPv6 add route unspecified      : 0
IPv6 add route other            : 1
IPv6 delete route total         : 7
```



```
IPv6 delete route destination : 7
IPv6 delete route source      : 0
IPv6 delete route gateway     : 0
IPv6 delete route unspecified : 0
IPv6 delete route other       : 0
Unspecified event             : 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 nexthop-list

```
show ipv6 nexthop-list
  details STRING
  STRING
```

Description

This command displays the next hop list settings for policy-based routing in IPv6 address. A next hop IP is the IPv4 or IPv6 address of an adjacent router or device with layer-2 connectivity to the managed device. The next hop list provides redundancy for the next hop devices by forwarding the traffic to a backup next hop device in case of failures. If the active next hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next hop on the list. For more information on this feature, see [ip nexthop-list on page 871](#).

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
details	Displays detailed next-hop settings for policy-based routing.
STRING	Displays the next-hop settings based on the next-hop list name.

Example

The following command displays the configuration settings for the one configured next hop list.

```
(host) [mynode] #show ipv6 nexthop-list
IPv6 Nexthop-List Entries
-----
Name      Dest  Preemptive Failover  Nexthop          Nexthop Dest
Nexthop  Priority
-----  -
-----
test      0x4402      Enabled      2032:1202:4072::2111  0x4421
1
test2    0x4403      Enabled      2006::3           0x4422
128
```

The output of this command displays the following information

Parameter	Description
Name	Name of the next hop list.
Dest	Destination prefix address.
Preemptive Failover	This column indicates whether preemptive failover is enabled or disabled. If preemption is enabled and a higher priority next hop becomes reachable again, packets are again forwarded to the higher priority next hop.
Nexthop	Next hop IPv6 address.
Nexthop Dest	Next hop destination prefix address.
Nexthop Priority	List of the IPv6 addresses of all next hop IPs, including the priority assigned to each device when the list was configured.

Related Commands

Command	Description
ip route	This command configures a static route on Mobility Conductor. (These routes can use a next hop list.)
ip nexthop-list	Configure next hop list settings for policy-based routing.

Command History

Version	Description
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ipv6 pd

```
show ipv6 pd
status
```

Description

Displays the prefix obtained by the PD client on uplink.

Example

The following example displays the status of the IPv6 prefix delegation.

```
(host)[mynode] #show ipv6 pd status
DHCPv6 PD Client is enabled
Uplink VLAN      : 100
Label           : site1
Prefix          : 2001:0:3::/48
65536 unique /64 prefixes are derivable from the acquired IA PD lease
Preferred lifetime 604800s, Valid lifetime 2592000s
Last request/renewal for the lease done at Thu Apr 14 04:46:15 2016
Lease expires at Sat May 14 04:46:15 2016
Downlink VLANs
-----
VlanId  Prefix
-----  -----
101     2001:0:3:12:1:2:3:4/64
```

Related Commands

Command	Description
ipv6 enable	This command enables IPv6 packet processing globally.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 ra

```
show ipv6 ra
  proxy
  status
```

Description

Displays the RA proxy server information and IPv6 RA.

Parameter	Description
proxy	Shows RA proxy server information.
status	Shows the status of IPv6 Router Advertisements.

Examples

The example below shows the IPv6 RA status on the VLAN interfaces .

```
(host) [mynode] #show ipv6 ra status
IPv6 RA Status
-----
VlanId  State    Prefix(es)
-----  -
1        enabled  2001:abcd:1234:dead::/64
220     enabled  2200:eab:feed:12::/64
230     enabled  2300:eab:feed::/64
7        enabled  2001:470:faca:2::/64
                2001:470:faca:3::/64
                2001:470:faca:4::/64

The example below shows the status of the IPv6 proxy RA:
(host) #show ipv6 ra proxy
IPv6 RA Proxy status: enabled
IPv6 RA Proxy interval: 600
```

Related Commands

Command	Description
ipv6 proxy-ra	This command configures an interval for proxy RA.

Command History

Release	Modification
ArubaOS 8.1.0.0	The <code>proxy</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 route

```
show ipv6 route
  counters
  static
```

Description

Displays the IPv6 routing table. This command displays static IPv6 routes configured on the managed device via the [ipv6 route](#) command. Use the [ipv6 default-gateway](#) command to set the default gateway to the IPv6 address of the interface on the upstream router or switch to which you connect the managed device.

Command	Description
counters	Displays the number of routes present, categorized by type.
static	Include this optional parameter to display only static IPv6 routes.

Examples

The examples below show the ipv6 address of routers and the VLANs to which they are connected.

```
(host) [mynode] #show ipv6 route
Codes: C - connected, O - OSPF, R - RIP, S - static
       M - mgmt, U - route usable, * - candidate default

Gateway of last resort is 2001::3 to network ::/128 at cost 1
S*   ::/0 [1/0] via 2001::3*
C    2001::/64 is directly connected, VLAN1
C    2010:abcd:1234:dead::/64 is directly connected, VLAN10

(host) [mynode] #show ipv6 route static
Gateway of last resort is 2001::3 to network ::/128 at cost 1
S*   ::/0 [1/0] via 2001::3*
```

Related Commands

Command	Description
ipv6 route	This command configures static IPv6 routes on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show ipv6 user-table

```
show ipv6 user-table
  ap-group <ap-group>
  ap-name <ap-name>
  authentication-method <dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web>
  bssid <A:B:C:D:E:F>
  debug
  essid <STRING>
  internal
  ip <A.B.C.D> [log]
  mac <A:B:C:D:E:F>
  mobile {[bindings][visitors]}
  name <STRING>
  phy-type {[a]|[b]}
  role <STRING>
  rows <NUMBER> <NUMBER>
  station <rows|unique>
  verbose <rows|unique>
```

Description

Displays IPv6 user table entries. You can filter the output based on various parameters are described in table.

Parameter	Description
ap-group <ap-group>	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
ap-name <ap-name>	Filter the output of this command by showing users connected to an AP with the specified AP name.
authentication-method	Filter the output of this command by the authentication method used for the device:
dot1x	Show data for devices using 802.1X authentication.
mac	Show data for devices using MAC authentication.
opensystem	Show data for devices using open (no) authentication.
psk	Show data for devices that do not use authentication but use a PSK for encryption.
stateful-dot1x	Show data for devices using stateful 802.1X authentication.
via-vpn	Show data for devices that authenticate using Aruba VIA.
vpn	Show data for devices using VPN authentication.

Parameter	Description
web	Show data for devices using captive portal authentication.
bssid	Displays entries in the IPv6 user-table that are associated to the specified BSSID.
debug	Displays entries in the IPv6 user-table that are in debug mode.
ssid	Displays entries in the IPv6 user-table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Displays internal IPv6 users.
ip <A.B.C.D>	Displays IPv6 users that match the specified IPv6 IP address.
log	Displays the log information for the specified IPv6 client.
mac	Displays users with the specified MAC address.
mobile	Displays list of mobile users in the IPv6 user table. The following filters are available for this parameter: <ul style="list-style-type: none"> ▪ bindings—list of users that have moved away from the current controller. ▪ rows—displays entries that match the specified row number. ▪ unique—displays unique entries in the IPv6 user-table. ▪ visitors—displays users that have associated with the current controller.
name	Displays IPv6 user table entries that match the specified name.
phy-type	Displays IPv6 user table entries that match a or b phy-type.
role	Displays IPv6 user table entries that match the specified role.
rows	Displays specific rows in the IPv6 user table. Enter the starting row number and the number of rows to be displayed.
station	Displays the station table information for the IPv6 user table entries.
verbose <rows unique>	Displays the complete IPv6 user table with all details.

Example

This example displays a list of users.

```
(host) [mynode] #show ipv6 user-table
Users
-----
IP                               MAC                               Name   Role   Age
(d:h:m)  Auth   VPN link  AP name  Roaming  Essid/Bssid/Phy
          Profile Forward mode  Type    Host Name
-----
-----
2010:eab::59ee:264a:a702:ca57  c0:14:3d:d9:e2:1b  salz   guest
00:04:30  802.1X          AP-105  Away   IPv6-dot1x-
7220/00:24:6c:11:88:40/g-HT  default  tunnel      Win 7
User Entries: 1/1
```

This example displays 802.1X authenticated users in the IPv6 user table.

```
(host) [mynode] #show ipv6 user-table authentication-method dot1x
Users
-----
IP                               MAC                               Name   Role
Age(d:h:m)  Auth   VPN link  AP name  Roaming  Essid/Bssid/Phy
          Profile
-----
-----
fe80::216:ceff:fe2c:b485          00:16:ce:2c:b4:85  Wing-A  logon
00:00:06  802.1X          00:0b:86:c1:0e:8c  Wireless Wing-
A/00:0b:86:90:e8:c0/g  default-dot1x
2003:d81f:f9f0:1001:617c:9151:6d25:f754  00:16:ce:2c:b4:85  Wing-A  logon
00:00:06  802.1X          00:0b:86:c1:0e:8c  Wireless Wing-
A/00:0b:86:90:e8:c0/g  default-dot1x
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the client in that row that authenticating using 802.1X
MAC	MAC address of the client.
Name	Name of the client.
Role	The role assigned to the client.
Age (d:h:m)	Total time that client is connected to controller.
Auth	Authentication type.
AP name	Name of the AP associated with the client.

Parameter	Description
Roaming	Current roaming status of the client.
Essid/Bssid/Phy	ESSID or BSSID or Phy to which the client is associated.
Profile	Displays the AAA profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show jitter

```
show jitter <probe_ip> <src_intf>
```

Description

This command displays the debug messages for the IPsec tunnel manager. This command should be executed from the managed device only.

Parameter	Description
<probe_ip>	IP address of a remote host to which the managed device is connected.
<src_intf>	Source interface VLAN of a remote host to which the managed device is connected.

Related Commands

Command	Description
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device up-links.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show keys

```
show keys [all]
```

Description

This command displays if optional keys and features are enabled or disabled on Mobility Conductor.

Parameter	Description
all	Include this optional parameter to display the status of all optional keys and features. If this parameter is omitted, the output displays the status of the most commonly used features and keys.

Example

The following example displays the status of the most commonly used keys and features on Mobility Conductor:

```
(host) [mynode] #show keys all
Licensed Features
-----
Feature                               Status
-----
Access Points                          10240
MUXes                                   Unlimited
External Servers                       Unlimited
xSec Users                              Unlimited
CIM Users                               Unlimited
Contexts                                Unlimited
3rd-party Remote APs                   Unlimited
RF Protect                              0
VPN Server Module                       16384
xSec Module                             0
Application-Acceleration Remote APs    Unlimited
Next Generation Policy Enforcement Firewall Module 10240
Advanced Cryptography                   0
WebCC                                    10240
Beta AP                                 0
MM                                       0
WLAN Switch                             ENABLED
RF Protect                              ENABLED
RF Director                             ENABLED
Policy Enforcement Firewall             ENABLED
Auto Radio Resource Alloc               ENABLED
Adaptive Radio Management               ENABLED
VPN Server                              ENABLED
Wired 802.1X                            ENABLED
```

Secure Access	ENABLED
Wired Grid Points	ENABLED
xSec Module	ENABLED
Remote AP VPN Termination	ENABLED
Location API	DISABLED
Mesh Visualization	DISABLED
Power Over Ethernet	DISABLED
Application Acceleration	DISABLED
Centralized Encryption	DISABLED
Policy Enforcement Firewall for VPN users	DISABLED
Advanced Cryptography	ENABLED
Maritime Regulatory Domain	DISABLED
X86 VM SKU Activate	DISABLED
WebCC	ENABLED
Beta AP	DISABLED

Related Commands

Command	Description
show license	View the license usage database (including the license key strings).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show lacp

```
show lacp
  summary
  sys-id
  <id> {counters|internal|neighbor}
```

Description

This command displays the Link Aggregation Control Protocol (LACP) configuration status.

Parameter	Description
summary	Displays summary of all LACP information and statistics.
sys-id	Displays LACP system ID.
<id>	Specify group ID. Range is 0-7.
counters	Enter the keyword counters to view the LACP traffic.
internal	Enter the keyword internal to view the LACP internal information.
neighbor	Enter the keyword neighbor to view the LACP neighbor information.

Example

This command returns the port priority and the MAC address (comma separated). In the example below, the port priority is the default value 32768 followed by the MAC address 00:0B:86:40:37:C0.

```
(host) [mynode] #show lacp sys-id
32768,00:0B:86:40:37:C0
```

The port uses the group number +1 as its “actor admin key”. By default, all the ports use the long timeout value (90 seconds).

```
(host) [mynode] #show lacp 0 neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting fast LACPDUs
        A - Device is in active mode P - Device is in passive mode
Partner's information
-----
Port    Flags  Pri  OperKey  State Num  Dev Id
-----
```

```
FE 1/1 SA 1 0x10 0x45 0x5 00:0b:86:51:1e:70
FE 1/2 SA 1 0x10 0x45 0x6 00:0b:86:51:1e:70
```

When a port, in a LAG, is disconnected (that is, the partner device is different than the other ports or the neighbor times out or can not exchange LACPDUs with the partner), the port status is displayed as **DOWN**. See the following example.

```
(host) [mynode] #show lacp 0 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting fast LACPDUs
       A - Device is in active mode P - Device is in passive mode
Port   Flags  Pri  AdminKey  OperKey  State Num  Status
-----
FE 1/1 SA    1    0x1       0x1      0x45  0x2  DOWN
FE 1/2 SA    1    0x1       0x1      0x45  0x3  UP
```

The “counters” option allows you to view LACP received (Rx) traffic, transmitting (Tx) traffic, data units (DU) received and transmitted by port.

```
(host) [mynode] #show lacp 0 counters
Port   LACPDUtx  LACPDURx  MarkrTx  MarkrRx  MrkrRspTx  MrkrRspRx
-----
FE 1/1  10         10         0         0         0           0
FE 1/2  12         12         0         0         0           0
```

Related Commands

Command	Description
lacp group	Enables LACP and configure on the interface.
lacp port-priority	Configures the LACP port priority.
show interface port-channel	Displays information for a specified port-channel interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show lc-cluster

```
show lc-cluster
  bucket [distribution {all|ssid <ssid-name>}]
  bucketmap [publish {counters}]
  exclude-vlan
  global-events
  group-membership
  group-profile
  gsm counters
  heartbeat counters
  history
  load distribution
  papi counters
  upgrade
  scheduled-upgrades
  vlan-probe
  <profile> {ap|controller|upgrade}
```

Description

Displays information related to vlan, membership, profile, heartbeat, and so on for a cluster. The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
bucket distribution all	Displays the current bucket distribution for all the ESSIDs.
bucket distribution ssid <ssid-name>	Displays the current bucket distribution for a specific ESSID.
bucketmap publish counters	Displays the details of the published bucketmap counters.
exclude-vlan	Displays a list containing vlans excluded from L2 Probing.
global-events	Displays cluster events.
group-membership	Displays the active cluster member of cluster profile
group-profile	Displays the cluster profile
gsm counters	Displays the counters pertaining to various GSM events
heartbeat counters	Displays the peer disconnection events statistics.
history	Displays cluster history.
load distribution	Displays the current load distribution

Parameter	Description
ap	Displays the current load distribution on the AP
client	Displays the current load distribution on the client
papi	Displays the cluster messaging related counters.
vlan-probe	Displays the Cluster VLAN Probe information.
<profile>	Displays the name of the cluster profile.
ap {details}	Displays the details of the APs in the cluster.
controller {details ip ipv6}	Displays the controllers details in the cluster. Use one of the following parameters: <ul style="list-style-type: none"> ▪ details—Displays the details of the controllers in the cluster. ▪ ip <ipv4_addr> [active {ap [details]}]—Displays the IP address details of the controllers in the cluster. ▪ ipv6 <ipv6_addr> [active {ap [details]}]—Displays the IPv6 address details of the controllers in the cluster.
upgrade	Displays the upgrade details of controllers and APs in the cluster. Use one of the following parameters: <ul style="list-style-type: none"> ▪ stats: Displays the statistics of the cluster upgrade. ▪ status: Displays the upgrade status of each controller and AP.
rap-public-ip	Displays the public IP address of the Remote AP cluster configured behind NAT.
scheduled-upgrades	Displays the status of all the clusters scheduled for an upgrade.

Example

An example output of the `show lc-cluster group-membership` command for a cluster running ArubaOS 8.11.0.0 or later versions.

```
Cluster Enabled, Profile Name = "test4nodecluster"
Redundancy Mode On
Active AP Load Balancing:YES
Active AP Rebalance Threshold:20%
Active AP Unbalanced Threshold:5%
Active AP Rebalance Count:50
Active AP Rebalance Timer:1 mins
```

```

Starting VRRP ID:99
VRRP Passphrase:*****
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
peer   10.17.65.34        128    L2-Connected CONNECTED (Leader, last HBT_
RSP 11

self   10.17.65.35         128    N/A CONNECTED (Member) peer   10.17.65.36
      128             N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer   10.17.65.37         128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer   10.17.65.38         128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)

```

An example output of the `show lc-cluster group-membership` command for a cluster running ArubaOS 8.10.0.0 or older versions.

```

Cluster Enabled, Profile Name = "test4nodecluster"
Redundancy Mode On
Active Client Rebalance Threshold:20%
Standby Client Rebalance Threshold:40%
Unbalance Threshold:5%
Active AP Load Balancing:YES
Active AP Rebalance Threshold:20%
Active AP Unbalanced Threshold:5%
Active AP Rebalance Count:50
Active AP Rebalance Timer:1 mins
Starting VRRP ID:99
VRRP Passphrase:*****
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
peer   10.17.65.34        128    L2-Connected CONNECTED (Leader, last HBT_
RSP 11

self   10.17.65.35         128    N/A CONNECTED (Member) peer   10.17.65.36
      128             N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer   10.17.65.37         128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer   10.17.65.38         128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)

```

An example output of the `show lc-cluster exclude-vlan` command.

```

#show lc-cluster exclude-vlan
-----
VLANs excluded from probing
-----
1

```

An example output of the `show lc-cluster group-profile` command for a cluster running ArubaOS 8.11.0.0 or later versions.

```
#show lc-cluster group-profile cluster_test
IPv4 Cluster Members
-----
CONTROLLER-IP  PRIORITY  MCAST-VLAN  VRRP-IP  VRRP-VLAN  VRRP-VLAN  GROUP-ID
RAP-PUBLIC-IP
-----
-----
10.17.65.34    128       0           0.0.0.0  0          200        0
10.10.10.11
10.17.65.35    128       0           0.0.0.0  0          200        0
10.10.10.12
Redundancy:Yes
```

An example output of the `show lc-cluster group-profile` for a cluster running ArubaOS 8.10.0.0 or older versions.

```
#show lc-cluster group-profile cluster_test
IPv4 Cluster Members
-----
CONTROLLER-IP  PRIORITY  MCAST-VLAN  VRRP-IP  VRRP-VLAN  VRRP-VLAN  GROUP-ID
RAP-PUBLIC-IP
-----
-----
10.17.65.34    128       0           0.0.0.0  0          200        0
10.10.10.11
10.17.65.35    128       0           0.0.0.0  0          200        0
10.10.10.12
Redundancy:Yes
Active Client Rebalance Threshold:20%
Standby Client Rebalance Threshold:45%
Unbalance Threshold:5%
```

An example output of the `show lc-cluster gsm` command.

```
#show lc-cluster gsm counters
Cluster GSM Channel Counters
-----
STA Channel: Adds >> 0
STA Channel: Deletes >> 0
STA Channel: Activates >> 0
STA Channel: Deactive and Dormant Deletes >> 0
Cluster STA Channel: Dormant Adds >> 0
Cluster STA Channel: Dormant Deletes >> 0
Cluster STA Channel: Dormant Section Update >> 0
Cluster STA Channel: Section Update >> 0
Cluster STA Channel: STA not found during Dormant Section Update >> 0
Cluster STA Channel: STA not found during Section Update >> 0
AP Channel: Adds >> 0
AP Channel: Deletes >> 0
Cluster AP Channel: Dormant Adds >> 0
Cluster AP Channel: Deactivates >> 0
Cluster AP Channel: Dormant Deletes >> 0
```

```

BSS Channel: Adds >> 0
BSS Channel: Deletes >> 0
BSS Channel: Section Update >> 0
BSS Channel: BSS not found during Section Update >> 0
Cluster BSS Channel: Dormant Adds >> 0
Cluster BSS Channel: Deactivates >> 0
Cluster BSS Channel: Dormant Deletes >> 0

```

An example output of the `show lc-cluster heartbeat` command.

```

#show lc-cluster heartbeat counters
Cluster Heartbeat Counters
-----
IPv4 Address          RES      RSR   MIS  HMPD LMRPD  IDPD CPDPD CDPD LMHINT
                   LTOD
-----
10.17.65.34    28147   28147   0   61    0    0    0    0   376 Thu
Jun 16 23:53:48 2016
10.17.65.36         0        0    0    0    0    0    0    0    0
10.17.65.37         0        0    0    0    0    0    0    0    0
10.17.65.38         0        0    0    0    0    0    0    0    0
-----PREAMBLE-----
RES    - REQ SENT
RSR    - RSP RCVD
MIS    - MISSES
HMPD   - HBT MISS PEER DEAD
LMRPD  - LINK MAP RCVD PEER DEAD
IDPD   - IPSEC DOWN PEER DEAD

```

An example output of the `show lc-cluster papi` command.

```

#show lc-cluster papi counters
Cluster PAPI Counters
-----
RX STM UP >> 1
RX STM DOWN >> 1
RX AUTH UP >> 0
RX AUTH DOWN >> 0
RX ISAKMPD UP >> 0
RX ISAKMPD DOWN >> 0
RX DDS UP >> 0
RX DDS DOWN >> 0
TX SOS CLUSTER ENABLE SUCCESS >> 2
TX SOS CLUSTER ENABLE FAIL >> 0
TX SOS CLUSTER DISABLE SUCCESS >> 1
TX SOS CLUSTER DISABLE FAIL >> 0
TX SOS CLUSTER PEER ADD SUCCESS >> 127
TX SOS CLUSTER PEER ADD FAIL >> 0
TX SOS CLUSTER PEER DEL SUCCESS >> 0
TX SOS CLUSTER PEER DEL FAIL >> 0

```

An example output of the `show lc-cluster load` command.


```
#show lc-cluster load distribution ap
Cluster Load Distribution for APs
-----
Type IPv4 Address      Active APs      Standby APs
-----
self   10.15.146.3          3              3
peer   10.15.146.4          1              3
peer   10.15.146.5          1              0
peer   10.15.146.6          1              0
Total: Active APs 6 Standby APs 6
```

```
#show lc-cluster load distribution client
Cluster Load Distribution for Clients
-----
Type IPv4 Address      Active Clients  Standby Clients
-----
self   10.15.146.3          0              0
peer   10.15.146.4          0              1
peer   10.15.146.5          0              0
peer   10.15.146.6          1              0
Total: Active Clients 1 Standby Clients 1
```

An example output of the `show lc-cluster vlan-probe` command.

```
#show lc-cluster vlan-probe status
Cluster VLAN Probe Status
-----
Type IPv4 Address      REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD
VLAN_FAIL CONN-TYPE START/STOP
-----
peer   10.17.65.34          248          0          372          0          372          248
0      L2 Conn          5/ 5
peer   10.17.65.36          0            0            0            0            0            0
0      N/A              0/ 49
peer   10.17.65.37          0            0            0            0            0            0
0      N/A              0/ 49
peer   10.17.65.38          0            0            0            0            0            0
0      N/A              0/ 49
```

An example output of the `show lc-cluster scheduled-upgrades` command.

```
show lc-cluster scheduled-upgrades
Cluster Scheduled Upgrade Status
-----
Profile To Version Partition ID AP Preload size Scheduled Time MD Timezone
-----
v4 8.4.0.0-mm-dev_65200 Default 100 Fri Jun 8 15:00:00 2018 Asia/Tokyo
```

An example output of the `show lc-cluster bucket distribution all` command.

```

#show lc-cluster bucket distribution all
Cluster Load Distribution for bucketmap
-----
Type IPv4 Address      Active Buckets Standby Buckets Ideal Active Buckets
Ideal Standby Buckets
-----
-----
ESSID AP_groupapsim300-PEAP
peer  192.168.192.8      43           43           43
      43
peer  192.168.192.2      43           43           43
      43
self  192.168.192.1      43           43           43
      43
peer  192.168.192.7      43           43           43
      43
peer  192.168.192.4      42           42           42
      42
peer  192.168.192.3      42           42           42
      42
(Node1) #

```

An example output of the `show lc-cluster bucket distribution essid <essid-name>` command.

```

#show lc-cluster bucket distribution essid AP_groupapsim300-PEAP
Cluster Load Distribution for bucketmap
-----
Type IPv4 Address      Active Buckets Standby Buckets Ideal Active Buckets
Ideal Standby Buckets
-----
-----
ESSID AP_groupapsim300-PEAP
peer  192.168.192.8      43           43           43
      43
peer  192.168.192.2      43           43           43
      43
self  192.168.192.1      43           43           43
      43
peer  192.168.192.7      43           43           43
      43
peer  192.168.192.4      42           42           42
      42
peer  192.168.192.3      42           42           42
      42

```

An example output of the `show lc-cluster bucketmap publish counters` command.

```

#show lc-cluster bucketmap publish counters

Cluster Bucket Map Publish Counters
-----

```

```

Bmap publish: JOIN >> 2
Bmap publish: Isolate Leader >> 1
Bmap publish: Prepare A-UAC periodic rebalance >> 18
Bmap publish: S-UAC->A-UAC move >> 22
Bmap publish: S-UAC Assign >> 22

```

Related Commands

Command	Description
lc-cluster group-profile	This command is used to configure the cluster group profile in the Mobility Conductor.
lc-cluster group-membership	This command configures the group-membership in each node. This command is used to enable the cluster membership on the managed devices.
show datapath cluster details	This show command displays heartbeat threshold values, datapath assignments, number of peers and peer data statistics.
show datapath cluster heartbeat counters	This command displays information related to cluster heartbeat counters.
show lc-cluster history	This command displays the history of the connection and disconnection events with a reason and the time stamp.

Command History

Release	Modification
ArubaOS 8.11.0.0	The following changes were introduced: <ul style="list-style-type: none"> ■ The <code>active-client-rebalance-threshold</code>, <code>standby-client-rebalance-threshold</code>, and <code>unbalance-threshold</code> fields were removed from the output of the <code>show lc-cluster group-membership</code> command. ■ The <code>bucket distribution all</code>, <code>bucket distribution essid <ssid-name></code>, and <code>bucketmap publish counters</code> parameters were added.
ArubaOS 8.7.0.0	The functionality of <code>heartbeat counters</code> parameter was modified.

Release	Modification
ArubaOS 8.5.0.0	The load balance thresholds were updated in the output and the Starting VRRP ID and VRRP Passphrase fields are added in the output.
ArubaOS 8.4.0.0	The parameter <code>scheduled-upgrades</code> and <code>rap-public-ip</code> were added.
ArubaOS 8.2.0.0	The parameter details of <code><profile></code> were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode or enable mode in the managed device.

show lc-cluster history

show lc-cluster history

Description

Displays the history of the connection and disconnection events with a reason and the time stamp.

Example

An example output of the show lc-cluster history command.

```
#show lc-cluster history
Cluster History
-----
-----LEGEND-----
HRPC  - HBT RCVD PEER CONN
HMPD  - HBT MISS PEER DEAD
LMRPD - LINK MAP RCVD PEER DEAD
IDPD  - IPSEC DOWN PEER DEAD
CPDPD - CRIT PROCESS DOWN PEER DEAD
CDPD  - CLUSTER DISABLED PEER DEAD
-----
TIME                IPv4 Address      STATUS      REASON
-----
Mon May 11 22:19:27 2020 10.16.147.131   CONNECTED   HRPC
Wed May 13 00:15:04 2020 10.16.147.131   DISCONNECTED HMPD
Wed May 13 00:17:18 2020 10.16.147.131   CONNECTED   HRPC
Wed May 13 01:34:28 2020 10.16.147.131   DISCONNECTED HMPD
Wed May 13 01:35:42 2020 10.16.147.131   CONNECTED   HRPC
Wed May 13 05:34:13 2020 10.16.147.132   CONNECTED   HRPC
Fri May 15 00:28:21 2020 10.16.147.132   DISCONNECTED LMRPD
Wed May 20 01:12:47 2020 10.16.147.132   CONNECTED   HRPC
(MD9) #show lc-cluster history
Cluster History
-----
-----LEGEND-----
HRPC  - HBT RCVD PEER CONN
HMPD  - HBT MISS PEER DEAD
LMRPD - LINK MAP RCVD PEER DEAD
IDPD  - IPSEC DOWN PEER DEAD
CPDPD - CRIT PROCESS DOWN PEER DEAD
CDPD  - CLUSTER DISABLED PEER DEAD
-----
TIME                IPv6 Address      STATUS
REASON
-----
Tue May 19 04:24:22 2020                2001:192:167:8::7
CONNECTED           HRPC
```

```
Tue May 19 04:24:22 2020
CONNECTED      HRPC
Tue May 19 04:27:25 2020
CONNECTED      HRPC
```

```
2001:192:167:8::8
2001:192:167:8::6
```

Related Commands

Command	Description
show datapath cluster details	This show command displays heartbeat threshold values, datapath assignments, number of peers and peer data statistics..
show datapath cluster heartbeat counters	This command displays information related to cluster heartbeat counters.
show lc-cluster	This command displays information related to vlan, membership, profile, heartbeat, and so on for a cluster.

Command History

Release	Modification
ArubaOS 8.11.0.0	Command updated to fix an example.
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode or enable mode in the managed device.

show lc-rap-pool

show lc-rap-pool <pool_name>

Description

This command displays the remote AP inner IP pool for cluster deployment.

Parameter	Description
pool_name	Name of the local IP pool to show.

Example

The output of the example below displays the Remote AP inner IPv4 and IPv6 pool that can be used for cluster deployment.

```
(host) [mynode] (config) #show lc-rap-pool rap-cluster
IP addresses used in pool rap-cluster
200.1.1.1-200.1.1.11
200.1.1.13
IPv6 addresses used in pool v6pool
fd00::1-fd00::b
fd00::d
IPv4 pool : Total - 12 IPs used - 88 IPs free - 100 IPs configured
IPv6 pool : Total - 12 IPs used - 243 IPs free - 255 IPs configured
LC RAP Pool Total Allocs/Deallocs/Reserves : 4/2/0
LC RAP Pool Allocs/Deallocs/Reserves(succ/fail) : 4/2/(22/0)
```

Related Commands

Command	Description
lc-rap-pool	This command is used to configure the Remote AP inner IPv4 pool for cluster deployment.
lc-rap-pool-v6	This command is used to configure the Remote AP inner IPv6 pool for cluster deployment.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output of the command was modified to display IPv6 address used in Remote AP inner pool.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show lcd-menu

```
show lcd-menu
```

Description

This command displays the current LCD Menu configuration on the managed device.

Example

The following example displays the output of the `show lcd-menu` command.

```
(host) [mynode] #show lcd-menu
lcd-menu
-----
Parameter                               Value
-----
menu maintenance upgrade-image partition0  enabled
menu maintenance upgrade-image partition1  enabled
menu maintenance upgrade-image            enabled
menu maintenance upload-config            enabled
menu maintenance factory-default          enabled
menu maintenance media-eject              enabled
menu maintenance reload-system            enabled
menu maintenance halt-system              enabled
menu maintenance                          enabled
menu                                       enabled
```

Related Commands

Command	Description
lcd-menu	This command allows you to enable or disable the LCD menu either completely or for specific operations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show lclist

```
show lclist
```

Description

This command displays the list of managed devices connected to Mobility Conductor.

Example

The following command displays the list of managed devices connected to Mobility Conductor.

```
(host) [mynode] #show lclist
All LC List
-----
IP Address      Name           Location      Model         Version
-----
Status
-----
-----
192.0.2.15     Standby-HQ     Building1.floor1  ArubaMM      8.0.0.0-svcs-
ctrl_55561    up
192.0.2.16     Corp-7240      Building1.floor1  Aruba7240    8.0.0.0-svcs-
ctrl_55561    up
192.0.2.17     Corp-7210      Building1.floor1  Aruba7210    8.0.0.0-svcs-
ctrl_55561    up
192.0.2.18     Corp-7220      Building1.floor1  Aruba7220    8.0.0.0-svcs-
ctrl_55561    up
192.0.2.19     Corp-VPNC      Building1.floor1  Aruba7010    8.0.0.0-svcs-
ctrl_55561    up
192.0.2.20     Corp-BOC1      Building1.floor1  Aruba7010    8.0.0.0-svcs-
ctrl_55561    up
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show license

```
show license
  aggregate
  asp
  box
  capacity-details
  client-table
  debug
  heartbeat
  key
  keys
  limits
  md-pefv-lic
  passphrase
  platform-limits
  pool-profile
  remote
  server-table
  summary
  verbose
```

Description

Displays the license table or Mobility Conductor passphrase.

Parameter	Description
<u>aggregate</u>	Displays the license aggregate table.
<u>asp</u>	Displays the Aruba Support Portal license.
<u>box</u>	Shows box license information.
capacity-details	Displays capacity license details on the device. NOTE: This option is valid only on 9240 controllers.
<u>client-table</u>	Displays license client-table entries
<u>debug</u>	Displays debug information.
<u>heartbeat</u>	Shows the license heartbeats.
<u>key</u>	Shows single license key's information
<u>keys</u>	Shows license keys information based on feature/license type.

Parameter	Description
limits	Enter the keyword limit to display the current license limits.
md-pefv-lic	Displays the MD PEFV license information.
passphrase	Issue the <code>show license passphrase</code> command to identify the Mobility Conductor passphrase. This passphrase is used in the licensing website to generate a Mobility Conductor (MM) license, or to generate a sharable license that can be added to Mobility Conductor license pools.
platform-limits	Displays the current platform license limits.
pool-profile	Shows license pool profile.
remote	Displays the license management remote command.
server-table	Displays License server-table entries
summary	Shows license summary information.
verbose	Displays the verbose output (deprecated, output is always verbose).

Example

An example output of the `show license` command.

```
(host)[node] # show license
License Table
-----
Key                               Installed   Expires   Flags
Service Type                      -----   -
-----
x7kbiBm5-3jI5MiBY-HVTAH/ci-11xPiKBV-dY8QGBMg-240 2010-01-21 Never
Access Points: 1024
21:00:22
itY24Hca-HSQlvJhi-yZtW6RB7-HGuBXzIq-N6hd6TNV-nZk 2010-01-21 Never E
120abg Upgrade: 128
21:01:03
oqdLOxZ6-+FS5DT2P-iNmtvc3o-NFyasYrO-ixGUrszE-4uo 2010-01-21 Never E
121abg Upgrade: 128
21:01:13
GIleLrCX-d8lxt3z5-vQC50n60-f31amOxu-Rf0uEoTn-qXQ 2010-01-21 Never E
124abg Upgrade: 128
21:01:22
```

```

ldsXG7ik-pj/HVm4t-Qt3541UC-3wzC+Efj-yn08g/HF-/Dg 2010-01-21 Never E
125abg Upgrade: 128
21:01:3
sJvaPL88-gWdDlMpj-LZMZ2YKK-2fU8NV61-XIH4wRk8-44I 2010-05-05 Never E
RF Protect: 512
08:51:57
QtemJpLj-Qm5D9WvK-8c9lbaL6-t2nU6/Pj-LSNd00FZ-tJo 2010-05-05 Never E
RF Protect: 1024
08:52:07
21:18:55
WNx6RasB-Qn9YVZ+5-giraq0Uy-aoIqS3as-FXmFh5dY-cSs 2010-01-21 Never E
xSec Module: 1024
21:20:56
u/GdQHWa-m4bzUCMC-ydMsWTif-hDMDajyB-qAlIMwnN-pGM 2010-01-25 Never E
Policy Enforcement Firewall for VPN users
18:44:19
F9dGNdjV-EmwLhqlI-oKMQQepZ-b9Jl3OB2-HQjwmc+r-vhI 2010-01-25 Never E
Next Generation Policy Enforcement Firewall Module: 128
18:44:19
License Entries: 11
Flags: A - auto-generated; E - enabled; R - reboot required to activate

```

The output of this command includes the following data columns:

Parameter	Description
Key	The license key.
Installed	The license installation date and time.
Expires	The date that your evaluation license expires is listed in this column. Permanent license will always have a "Never" in this column. Expired evaluation licenses will also be indicated in this column.
Flags	This column displays the status of your license. The legend for this column appears at the bottom of the display output. They are: A: The license is auto-generated. E: The license is fully enabled. R: You must reboot your controller to fully enable this license. M: The license is activated using Master Token Key.
Service Type	The license name (feature).

Related Commands

Command	Description
show keys	This command displays if optional keys and features are enabled or disabled on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.6.0.0	The flag M was introduced.
ArubaOS 8.0.1.0	The <code>passphrase</code> parameter is introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show license aggregate

```
show license aggregate
pool
```

Description

Display the total number of licenses of each license type in all Mobility Conductor licensing pools. Execute this command from any configuration node in the Mobility Conductor CLI to view the licenses in the global licensing pool and any local license pools, as well as the number of clients using each pool.

Example

The following example displays output of the `show license aggregate` command.

```
(host)[node] # show license aggregate
Aggregate License Table for pool /
-----
Hostname      IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR
WebCC
-----
-----
From Server   2002::2           6   3   0           0           0
0

Last update (secs. ago)
-----
60

Total no. of clients: 0
Aggregate License Table for pool /SC
-----
Hostname      IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR
WebCC
-----
-----
From Server   2002::3           128 128 128           64           16
16

Last update (secs. ago)
-----
60
Total no. of clients: 20

Aggregate License Table for pool /India
-----
Hostname      IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR
WebCC
```


Parameter	Description
<code>Last update (secs. ago</code>	Time, in seconds, that has elapsed since the licensing table on Mobility Conductor was updated.
<code>Total number of clients</code>	This value indicates the total number of clients using licenses from the licensing pool.

Related Commands

Command	Description
<code>show license key</code>	Display information about a specific license key.
<code>show license keys</code>	Display information about all installed license keys.
<code>show license box</code>	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.6.0.0	The output of the command also displayed the IPv6 address under <code>IP address</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license asp

```
show license asp
  stale
  unallocated-lic
```

Description

Displays Aruba Support Portal information.

Parameter	Description
stale	Displays stale ASP licenses.
unallocated-lic	Displays the Aruba Support Portal unallocated available license count.

Example

The following example displays output of the `show license asp stale` command.

```
(host)[node] # show license asp stale
```

The following example displays output of the `show license asp unallocated-lic` command.

```
(host)[node] # show license asp unallocated-lic
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license box

```
show license box remote
  remote-ip-addr <ip-addr>
```

Description

Display the device-specific licenses used by a remote managed device. Also, execute this command from the CLI of a managed device to view license limits applied to that managed device from its licensing pool.

Parameter	Description
remote remote-ip-addr <ip-addr>	IP address of the managed device.

Example

The following example displays output of the `show license box remote remote-ip-addr <ip-addr>` command.

```
Box Licenses Table
-----
Key                               Feature
Expiration  Status
---          -
-----
cvK33n5l-MeXuHi7N-gRyIa4As-Gh  X86 VM SKU Activate
Never          E/Active
V3rBYtzd-hOtVXuKi-WZeEYJU1-9k  Policy Enforcement Firewall for VPN users
Never          E/Active
```

The output of this command includes the following data columns:

Parameter	Description
Key	License key on the managed device.
Feature	Licensing feature enabled by the license key.
Expiration	This field displays the expiration date for evaluation or subscription licenses.
Status	Current status of the license.

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Conductor licensing pools.
show license key	Display information about a specific license key.
show license keys	Display information about all installed license keys.

Command History

Release	Modification
ArubaOS 8.0.1.0	The <code>remote remote-ip-addr</code> parameter was introduced, and the <code>remote ip-addr</code> parameter was deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license client-table

```
show license client-table
```

Description

Execute this command from the CLI of a managed device to view license limits applied to that managed device from its licensing pool.

Example

The following example displays output of the `show license client-table` command.

```
(host)[node] #show license client-table
Built-in limit: 0
License Client Table
-----
Service Type          System Limit  Server Lic.  Used Lic.  Remaining Lic.
FeatureBit
-----
Access Points         499           250           10          240
enabled
Next Gen PEF Module  499           250           10          240
enabled
RF Protect            499           0             0           0
disabled
Adv Cryptography     999999        0             0           0
disabled
WebCC                 499           250           10          240
enabled
MM-VA                 500           495           5           495
enabled
MC-VA-RW              499           0             0           0
enabled
MC-VA-EG              499           0             0           0
enabled
MC-VA-IL              499           0             0           0
enabled
MC-VA-JP              499           0             0           0
enabled
MC-VA-US              499           0             0           0
enabled
VIA                   499           0             0           0
enabled
```

The output of this command includes the following data columns:

Parameter	Description
Service Type	Type of license on the managed device.
System Limit	The maximum number of licenses supported by the man platform.
Server Lic.	Number of licenses available for use by the licensing client. NOTE: This number is limited by the total license capacity of the managed device platform. A managed device cannot use more licenses than is supported by that managed device platform, even if additional license are available.
Used Lic.	Total number of licenses of each license type used by the managed device.
Remaining Lic.	Total number of remaining licenses available in the licensing pool.
Feature Bit	This column indicates whether these license features are enabled or disabled. For more information about enabling a sharable license, see license-pool-profile-root .

Related Commands

Command	Description
show license aggregate	This command is used to view additional statistics for the licenses in each license pool.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output of this command displays information for VIA licenses introduced in ArubaOS 8.2.0.0.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on managed devices.

show license debug

```
show license debug
  auth-feature-bits
  feature-bits
```

Description

Displays a summary of Mobility Conductor's/Mobility Conductor's licensing role and IP address.

Parameter	Description
auth-feature-bits	Displays feature bits at auth for this controller.
feature-bits	Displays cached license feature bits for this controller

Example

The following example shows the output of the `show license debug` command.

```
(host)[node] # show license debug
Summary of licensing state
Centralized Licensing: Enabled
Switch Role: Master/ Conductor
License Role: License Client
Master/Conductor IP: 10.9.217.71
Master/Conductor IPv6: 2002::1
Switch IP: 10.16.16.160
Switch IPv6: 2002::2
License Server IP: 10.9.217.71 (or 2002::1 as configured)
```

The output of this command includes the following data columns:

Parameter	Description
Centralized licensing	Shows if centralized licensing is enable or disabled.
Switch Role	Role of the device using the configuration on which this command is run.
License Role	Licensing role of the controller on which this command is run. Mobility Conductor can be a licensing client or a licensing server. Managed devices can be licensing clients only.
Master/Conductor IP	IPv4 address used by Mobility Conductor. If a Mobility Conductor redundant pair is using VRRP, this parameter displays the VRRP virtual IP address.

Parameter	Description
Master/Conductor IPv6	IPv6 address used by Mobility Conductor.
Switch IP	IPv4 address assigned to the device using the configuration on which this command is run.
Switch IPv6	IPv6 address assigned to the device using the configuration on which this command is run.
License Server IP	Mobility Conductor IP address.

The following example shows the output of the `show license debug feature-bits` command.

```
(host)[node] # show license debug feature-bits

Cached feature bits
-----
FeatureBit                               LicType  Status
-----
REMOTE_AP                                 AP        Enabled_
Enabled_49_49
SECURITYGW                                PEFNG     Enabled_
Enabled_49_49
IDS                                         RFP       Enabled_
Enabled_49_49
BSEC                                        ACR       Enabled_
Enabled_32_32
WEBCC                                       WEBCC     Enabled_
Enabled_0_0
MCR                                         MCR       Enabled_
Enabled_50_50
MC-VA-RW                                   MC-VA-RW  Enabled_
Enabled_0_0
MC-VA-EG                                   MC-VA-EG  Enabled_
Enabled_0_0
MC-VA-IL                                   MC-VA-IL  Enabled_
Enabled_0_0
MC-VA-JP                                   MC-VA-JP  Enabled_
Enabled_0_0
MC-VA-US                                   MC-VA-US  Enabled_
Enabled_0_0
VIA                                         VIA       Enabled_
Enabled_0_0
```

The following example shows the output of the `show license debug auth-feature-bits` command.

```
(host)[node] # show license debug auth-feature-bits
```

```

License Debug - Auth Feature Bits
-----
Name                                     Value
----                                     -
Firewall License                         1

WLAN Switch                             Enabled
RF Protect                               Enabled
RF Director                              Enabled
Policy Enforcement Firewall              Enabled
Remote APs                               Enabled
External Services Interface              Disabled
Client Integrity Module                  Disabled
.
.
.
Licence Limits

Access Points                            49
Remote Access Points                     49
MUXes                                    16777215
External Servers                         16777215
xSec Users                               16777215
CIM Users                                16777215
Ortronics Access Points                  0
Contexts                                 16777215
.
.
.

```

Related Commands

Command	Description
show license aggregate	This command is used to view additional statistics for the licenses in each license pool

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	The command output displayed the following new parameters:

Release	Modification
	<ul style="list-style-type: none"> ■ Master IPv6 ■ Switch IPv6
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor and managed devices.

show license heartbeat stats

```
show license heartbeat stats
```

Description

Display the license heartbeat statistics between the centralized licensing server and the license client. If your deployment uses the centralized licensing feature, issue this command from the CLI of a centralized licensing server to view heartbeat requests to and responses from each licensing client associated to that licensing server. If you issue this command from a licensing client, the output displays information for that one client only.

Example

The following example displays output of the `show license heartbeat stats` command issued from the licensing server.

```
(host)[node] #show license heartbeat stats
License Client Heartbeat Table
-----
Server IP Address  Mac Addr           HB Req   HB Resp   Total Missed
Last Update (secs. ago)
-----
10.17.52.195      00:0c:29:bb:0f:8f  13843    13836     7
2
License Server Heartbeat Table
-----
Client IP Address  Mac Addr           HB Req   HB Resp   Total Missed
Last Update (secs. ago)
-----
10.17.24.22       00:1a:1e:00:d9:40  13844    13843     1
28
```

The output of this command includes the following data columns for License Heartbeat Table and License Server Heartbeat Table:

Parameter	Description
Server IP address	IPv4 or IPv6 address of the licensing client.
Mac Addr	MAC address of the licensing client.
HB Req	Heartbeat requests sent from the licensing client.
HB Resp	Heartbeat responses received from the license server.

Parameter	Description
Total Missed	Total number of heartbeats that were not received by the licensing client.
Last Update	Number of seconds elapsed since the licensing client last sent a heartbeat request.

Related Commands

Parameter	Description
show license aggregate	View additional statistics for license usage on the licensing server master/ conductor .

Command History

Release	Modification
ArubaOS 8.6.0.0	The command output also displayed IPv6 address information in <code>IP Address</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on centralized licensing master/ conductor or licensing client controllers.

show license key

```
show license key <key>
```

Description

Display information about a specific evaluation or subscription license key. Issue this command from the Mobility Conductor CLI to view the status of an installed evaluation or subscription license key.

Parameter	Description
<key>	License key

Example

The following example displays output for the `show license key` command. In this example, the output has been modified to appear in two separate sections. In the actual CLI, this output appears in a single, long row.

```
(host)[node] #show license key eLNB351-21F-3WE

Key Attributes:
-----
Feature  Type          Expiration          GraceExpiration      TotalCount
-----  -
WebCC    Subscript  2017-05-03 10:36:54  2017-08-31 10:36:54  10

AvailableForAllocation  Status
-----  -----
10                      E/Active
Flags: E - enabled; R - reboot/activation key required to activate; D - Not
enabled on Local Controller
```

The output of this command includes the following data columns:

Parameter	Description
Key	License key
Feature	Feature type supported by the license key
Type	ArubaOS supports the permanent , evaluation or subscription license types, but this command displays information about evaluation and subscription licenses only.

Parameter	Description
Expiration	The expiration date for the subscription or evaluation license key.
GraceExpiration	The grace period for which a subscription remains fully active after the subscription key expiration date.
TotalCount	The total number of licenses supported by the license key.
AvailableforAllocation	The total number of licenses that are still available for allocation
Status	This column shows the current status of the license, including whether it is active or expired, and whether that licensing feature is enabled on Mobility Conductor or the stand-alone controller.

Related Commands

Command	Description
<u>show license aggregate</u>	Display the total number of licenses of each license type in all Mobility Conductor licensing pools.
<u>show license keys</u>	Display information about all installed license keys.
<u>show license box</u>	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license keys

```
show license keys
  [feature-type acr|ap|mc-va-eg|mc-va-il|mc-va-jp|mc-va-rw|mc-va-
  us|pefng|rfp|acr|xsc| [webc|mm]
  [license-type perm|eval|subscript|non-perm]
```

Description

Display information about all license keys installed on Mobility Conductor. Issue this command from the Mobility Conductor CLI to view the status of an installed license keys.

Parameter	Description
Feature-type	View a list of license keys for the specified feature type.
acr	View Advanced Cryptography (ACR) licenses.
ap	View AP licenses.
mc-va-eg	View MC-VA-EG license type information for Egypt.
mc-va-il	View MC-VA-IL license type information for Israel.
mc-va-jp	View MC-VA-JP license type information for Japan.
mc-va-rw	View MC-VA-RW license type information for rest of the world (all other countries)
mc-va-us	View MC-VA-US license type information for United States.
mm	View MM licenses for Mobility Conductor.
pef	View Policy Enforcement Firewall (PEF) licenses.
rfp	View RF Protect licenses.
xsc	View xSec licenses.
License-type	View a list of license keys of the specified license type.
perm	Display a list of permanent licenses.
eval	Display a list of evaluation licenses.
subscript	Display a list of subscription licenses .
non-perm	Display a list of non-permanent licenses (evaluation and subscription).

Example

The following example displays output for the `show license keys` command. In this example, the output has been modified to appear in two separate sections. In the actual CLI, this output appears in a single, long row.

```
(host)[node]#show license keys
License Keys info
-----
Key      Feature  Type      Expiration      GraceExpiration
TotalCount
-----
-----
7eWKHB6 PEFNG    Perm      Never           N/A             500
Ryw+Sau AP      Perm      Never           N/A             500
aHfQ8hZ ACR      Eval      2016-06-02 11:17:18      N/A             64
eLNBA35 WebCC    Subscript 2017-05-03 10:36:54      2017-08-31 10:36:54 10

AvailableForAllocation  Status
-----
450                      E/Active
450                      E/Active
64                       E/Expires in 29 days
10                       E/Active
```

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Conductor licensing pools.
show license key	Display information about a specific license key.
show license box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.2.0.0	The following parameters under <code>feature-type</code> were added:

Release	Modification
	<ul style="list-style-type: none"> ■ mc-va-eg ■ mc-va-il ■ mc-va-jp ■ mc-va-rw ■ mc-va-us
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license limits

```
show license limits
```

Description

Displays current license limits.

Example

The following example displays output of the `show license limits` command.

```
(host) [mynode] #show license limits
License Limits
-----
Limit  Value
-----  -----
49     Access Points
16     RF Protect
0      120abg Upgrade
0      121abg Upgrade
0      124abg Upgrade
0      125abg Upgrade
49     Next Generation Policy Enforcement Firewall Module
0      Advanced Cryptography
0      Service provider AP
49     WebCC
0      Beta AP
50     MM-VA
0      MC-VA-RW
49     MC-VA-EG
0      MC-VA-IL
0      MC-VA-JP
0      MC-VA-US
0      VIA
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license md-pefv-lic

```
show license md-pefv-lic
```

Description

Displays MD PEFV license information.

Example

The following example displays output of the `show license md-pefv-lic` command.

```
(host)[node] # show license md-pefv-lic
MD PEFV Status
-----
MAC                PEFV Installed
---                -
00:0b:86:b7:3a:07  N
20:4c:03:02:27:e0  N
00:0b:86:b7:3e:1f  N
20:4c:03:02:24:60  N
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license passphrase

show license passphrase

Description

Display the Mobility Conductor passphrase used to generate licenses for a Mobility Conductor deployment. Issue this command for a network where the Mobility Conductor software is installed on a VM.



This command is not supported on stand-alone controllers, the Mobility Conductor appliance or managed devices.

Example

```
(host)[node] #show license passphrase  
5I0N3bI6-exkTWLkq-P05tfofQ-d6NvLJR91
```

Related Commands

Command	Description
show inventory	Display the Mobility Conductor serial number used to generate licenses for a Mobility Conductor deployment.
product serial-number	This command configures the product serial-number for a managed device on a Virtual Machine (VM).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and config mode on Mobility Conductor.

show license platform-limits

show license platform-limits

Description

Display the licensing limits for Mobility Conductor or the controller platform upon which this command is issued. To view licensing limits for Mobility Conductor managed devices, you must access the CLI of that specific node.



The output of this command displays limits for currently supported licenses, as well as limits for deprecated license types no longer supported by this software version.

Example

The output of the following command displays platform limits for all licenses supported by Mobility Conductor.

```
(host)[node] #show license platform-limits
License Platform Limits
-----
Limit   Value
-----  -
999999  Access Points
999999  Remote Access Points
999999  Ortronics Access Points
999999  Outdoor Mesh Access Points
999999  Wireless Intrusion Protection Module
999999  VPN Service Module
4096    xSec Users
999999  Indoor Mesh Access Points
999999  120abg Upgrade
999999  121abg Upgrade
999999  124abg Upgrade
999999  125abg Upgrade
999999  Policy Enforcement Firewall Module
999999  Advanced Cryptography
0       SAP
999999  WebCC
999999  Beta AP
```

The following example displays platform limits for all licenses supported by a 7005 controller.

```
(host)[node] #show license platform-limits
License Platform Limits
-----
Limit   Value
```



```

-----
16      Access Points
16      Remote Access Points
16      Ortronics Access Points
32      Outdoor Mesh Access Points
16      Wireless Intrusion Protection Module
4096    VPN Service Module
4096    xSec Users
32      Indoor Mesh Access Points
16      120abg Upgrade
16      121abg Upgrade
16      124abg Upgrade
16      125abg Upgrade
16      Policy Enforcement Firewall Module
4096    Advanced Cryptography
0       SAP
16      WebCC
16      Beta AP

```

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Conductor licensing pools.
show license key	Display information about a specific license key.
show license box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license pool-profile

```
show license pool-profile
  root
  <pool>
```

Description

Use this command to display a license profile for the pool.

Parameter	Description
root	Show license profile for the root pool.
<pool>	Show license pool for the pool specified.

Examples

```
(host)[node] (config) ##show license pool-profile root

License Profile Summary For Root Pool
-----
Feature      Enable  TotalInstalledCount  AvailableCount
-----
AP           Yes    384                  384
PEFNG       Yes    128                  128
RFP         Yes    384                  384
ACR         Yes    32                   32
WebCC       No     0                    0
MM          Yes    500                  500
MC-VA-RW    No     0                    0
MC-VA-EG    No     0                    0
MC-VA-IL    No     0                    0
MC-VA-JP    No     0                    0
MC-VA-US    No     0                    0
VIA         No     0                    0
```

Related Commands

Version	Description
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

show license remote

```
show license remote
  remote-ip-addr
```

Description

Displays Aruba Support Portal information.

Parameter	Description
remote-ip-addr	Use this command to manage license remotely.

Example

The following example displays output of the `show license remote remote-ip-addr` command.

```
(host)[node] # show license remote remote-ip-addr 10.1.1.1
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license server-table

show license server-table

Description

Display the license server table for each licensing pool as it appears on the centralized licensing server.

If your deployment uses the centralized licensing feature, issue this command from the CLI of a centralized licensing server to view licensing counts for each supported license type.

Example

The following example displays part of the output of the `show license server-table` command issued from a licensing server. The complete output displays a separate table for each licensing pool.

```
(host) [node] #show license server-table
License Server Table for pool /
-----
Service Type          PoolSize  ExpiredLic  ActualPoolSize  UsedLic
RemainingLic  Warnings  FeatureBit
-----
-----
Access Points          2337      547         1790             0       1790
    Some licenses expired
Next Gen PEF Module   419       419         0                0        0
    Some licenses expired
RF Protect             9864      32          9832             0       9832
    Some licenses expired
xSec Module            0         0           0                0        0
    None
Advanced Cryptography 254       0           254             0       254
    Some licenses expiring
WebCC                  0         0           0                0        0
    None
MM-VA                  13750     10500       3250             0       3250
    Some licenses expired
MM-VA                  500       0           500             5       495
    None
MC-VA-RW               0         0           0                0        0
    None
MC-VA-EG               0         0           0                0        0
    None
MC-VA-IL               0         0           0                0        0
    None
MC-VA-JP               0         0           0                0        0
    None
MC-VA-US               0         0           0                0        0
    None
```

VIA	0	0	0	0	0
None			enabled		

The output of this command includes the following data columns:

Parameter	Description
ServiceType	Type of license on the licensing server.
PoolSize	The total number of licenses assigned to that licensing pool. This number includes both expired and active licenses.
ExpiredLic	Number of expired licenses for each license type.
ActualPoolSize	The total number of active licenses currently available for devices and users in the selected license pool. The <code>ActualPoolSize</code> value is the total number of licenses in the pool (<code>PoolSize</code>) value minus the expired licenses (<code>ExpiredLic</code>).
UsedLic	Total number of licenses of each license type reported as used by the licensing clients or licensing server.
RemainingLic	Total number of remaining licensing available in the licensing table.
Warnings	This column displays warnings if licenses have expired, or if licenses used on a per-session basis are no longer sufficient to support the client demand.
FeatureBit	This column indicates whether these license features are enabled or disabled. For more information about enabling a sharable license, see license-pool-profile-root .

Related Commands

Command	Description
show license aggregate	This command is used to view additional statistics for the licenses in each license pool.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output of this command displays information for VIA licenses introduced in ArubaOS 8.2.0.0.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license summary

show license summary

Description

Shows license summary information.

Example

The following example displays output of the `show license summary` command.

```
(host) [mynode] #show license summary
License Summary
-----
License   Description                               Status           Expiration
Total Installed
-----
-----
AP        Access Points                             Not Licensed     Not Licensed    0
PEFNG     Policy Enforcement Firewall                Not Licensed     Not Licensed    0
RFP       RF Protect (WIP, Spectrum, Multi-zone)    Not Licensed     Not Licensed    0
ACR       Advanced Cryptography                     Not Licensed     Not Licensed    0
WebCC     Web Content Classification                 Not Licensed     Not Licensed    0
MC-VA-RW  Controller Virtual Appliance (RW)         Not Licensed     Not Licensed    0
MC-VA-EG  Controller Virtual Appliance (EG)         Not Licensed     Not Licensed    0
MC-VA-IL  Controller Virtual Appliance (IL)         Not Licensed     Not Licensed    0
MC-VA-JP  Controller Virtual Appliance (JP)         Not Licensed     Not Licensed    0
MC-VA-US  Controller Virtual Appliance (US)         Not Licensed     Not Licensed    0
VIA       VIA VPN Client (Session-based)            Not Licensed     Not Licensed    0
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license verbose

show license verbose

Description

Displays verbose output.

Example

The following example displays the output of the `show license verbose` command.

```
(host) [mynode] #show license verbose
License Table
-----
Key
      Installed          Expires(Grace period expiry)  Flags  Service
Type
---
-----
---
Koo6papL-8W6V9O86-tIp7/tlp-hUvyqH6S-2D+uw9rw-s54KuhPJ-s4gklJam-yrdbp9wa-
k5ZfCizI-23c  2020-02-09 23:13:33  Never          E      VIA:
4000
xXzdQjvh-8qDFKa2A-U0Vfa9/m-kgWiuHuf-qHQ8XZrX-6WlwY+8y-1rCRmr4Y-xjbCYZ1E-
3nH4qViX-5Gk  2020-02-09 23:13:55  Never          E      MM-
VA: 5000
cUELb+Mk-VURnWkMK-sW5v5wzh-JJGMg36f-DKGCEAy0-xSJ/0Ypl-he0HJih3-j0AxKVKx-
t/EUyWSs-G1c  2020-02-09 23:13:33  Never          E
Access Points: 4000
E0OmCelY-3u3kDsaI-3a9JgnYH-nwPa7+Di-siMmJoEq-4bmgCves-CCQJNSqy-DO5c/NG+-
6p33oYE+-7a0  2020-02-09 23:13:33  Never          E      Next
Generation Policy Enforcement Firewall Module: 4000
xP4lnorX-CzBhuuLL-7vYQnA8y-/VwduFmB-KSCbmUvk-LfXat955-Pd9LZ1Vp-ZYh0F/mE-
NrizsT44-LDI  2020-04-06 02:16:29  Never          E      MM-
VA: 5000
mUecDQgr-tJrSCDJD-hWOA0aug-RSg8N9P8-DkNAQU1S-+aXcCJju-j0np27qr-vIkqepQ1-
y6ca12o1-mJg  2020-04-06 02:16:55  Never          E
Access Points: 5000
0MhgFCGB-luxqB6DB-NS87PqST-LAYX3a9B-GUjbXnC9-qSjPQTgk-MIbWNWk2-cGQ5yc/1-
L1twqFO4-kvs  2020-04-06 02:17:12  Never          E      RF
Protect: 5000
pZ9/pRcW-3OmT5oGu-CuX2NGwM-fY6dht5n-XaLv6wn5-iaXWjok0-HmvQt53U-RTDU5Q3E-
JGx2Rz+B-bqY  2020-04-06 02:17:33  Never          E      Next
Generation Policy Enforcement Firewall Module: 5000
QQ5ZyWx+-DvJXR2Vg-dk0h6M/X-tEXD1ZuL-PxbVnkCS-VYk8Kpj0-AoOYU3GN-vta9kfBL-
AEuMUqz0-5G4  2020-02-09 23:13:33  Never          E      RF
Protect: 4000
3b9D4Dhx-4eWirtf7-R+/Yvqtr-e00XdFz3-M8QORm5v-w6uTRwsz-Az3hloda-WCe7n9XW-
vOT4eeey-Tlk  2020-07-15 00:21:48  Never          E      MC-
VA-US: 50
License Entries: 10
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Conductor.

show license-pool-profile

```
show license-pool-profile [<profile>]
```

Description

Use this command to display a list of license pools, or display the licenses allocated for a specific pool. All managed devices associated to the same Mobility Conductor can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Conductor. However, ArubaOS also allows you to create individual licensing pools at a configuration node, allowing managed devices below that node to share licenses amongst themselves but not with other managed devices.

Parameter	Description
<profile>	<p>(Optional) The name of the profile for which you are creating a local license pool, for example, Northwest. The profile name is limited to 63 characters.</p> <p>NOTE: In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the <code>license-pool-path</code> parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less.</p>

Starting in ArubaOS 8.1, the `license-pool-path` parameter displays the license pool path for the profile, up to 255 characters, for example, `/USA/northwest`.

If you upgrade a legacy ArubaOS deployment to ArubaOS 8.1 or later, the `license-pool-path` parameter is automatically derived from the `license-pool-profile <profile>` name.

You must use the `license add` command to add license keys to the Mobility Conductor before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device, then issue the `license-pool-profile-root` command to enable licensing features on Mobility Conductor.



Examples

```
(host)[node] (config) #show license-pool-profile v6cluster

License pool profile "v6cluster"
-----
Parameter                               Value
-----
```

```

License pool path /md/v6cluster-1
AP permanent licenses 600
AP expiry licenses N/A
PEFNG permanent licenses 600
PEFNG expiry licenses N/A
RFP permanent licenses N/A
RFP expiry licenses N/A
ACR permanent licenses N/A
ACR expiry licenses N/A
WebCC expiry licenses N/A
WebCC subscription licenses N/A
VIA permanent licenses N/A
VIA expiry licenses N/A
MM permanent licenses 600
MM expiry licenses N/A
MC-VA Egypt permanent licenses N/A
MC-VA Egypt expiry licenses N/A
MC-VA Israel permanent licenses N/A
MC-VA Israel expiry licenses N/A
MC-VA Japan permanent licenses N/A
MC-VA Japan expiry licenses N/A
MC-VA USA permanent licenses N/A
MC-VA USA expiry licenses N/A
MC-VA Rest of the world permanent licenses N/A
MC-VA Rest of the World expiry licenses N/A

```

Parameter	Description
license-pool-path <license-pool-path>	<p>The name of the profile , for example, Northwest. The profile name is limited to 63 characters.</p> <p>NOTE: In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the <code>license-pool-path</code> parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less.</p>
AP Permanent Licenses AP Expiry License	These two fields show the numbers of permanent and temporary AP licenses.
PEFNG Permanent Licenses PEFNG Expiry License	These two fields show the numbers of permanent and temporary Next Generation Policy Enforcement Firewall (PEFNG) licenses.
RFP Permanent Licenses RFP Expiry License	These two fields show the numbers of permanent and temporary RF Protect (RFP) licenses.
ACR Permanent Licenses ACR Expiry License	These two fields show the numbers of permanent and temporary ArubaOS Advanced Cryptography (ACR) licenses .

Parameter	Description
WebCC Permanent Licenses WebCC Expiry License	These two fields show the numbers of permanent and temporary Web Content Classification (WebCC) licenses.
VIA Permanent Licenses VIA Expiry License	These two fields show the numbers of permanent and temporary Virtual Intranet Access (VIA) licenses.
MM Permanent Licenses MM Expiry License	These two fields show the numbers of permanent and temporary Mobility Conductor licenses in pool.
via-licenses	VIA licenses support Virtual Intranet Access (VIA) or 3rd party VPN client. VIA licenses are not consumed for site-to-site VPNs. If a managed device or standalone controller has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that device.
webcc-licenses	Add WebCC licenses to the selected pool. The Web Content Classification (WebCC) license is a subscription-based, per-AP license.
eval	(Optional) Include this keyword to add an evaluation license.
<num>	Number of licenses supported by the license key.

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.

Command History

Version	Description
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

show license-pool-profile root

```
show license-pool-profile root
```

Description

Use this command to determine the license types that are enabled and sharable via the root licensing profile. All managed devices associated to the same Mobility Conductor can share a pool of licenses that comprises of all the sharable licenses added to the Mobility Conductor. However, ArubaOS also allows you to create individual licensing pools at a configuration node that allows managed devices below the node to share licenses amongst themselves but not with other managed devices.



You must use the `license add` command to add license keys to the Mobility Conductor before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device, then issue the `license-pool-profile-root` command to enable licensing features on Mobility Conductor.

Examples

```
(host) ^[mynode] (config) #show license-pool-profile-root
License root(/) pool profile
-----
Parameter                Value      Set
-----                -
enable PEFNG feature     Enabled
enable RFP feature       Enabled
enable XSEC feature      true
enable ACR feature       true
enable WebCC feature     true
```

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on the controller.

Command History

Version	Description
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Enable and config mode on Mobility Conductor.

show license-usage

```
show license-usage
  acr
  ap
  capacity
  client [pool <pool>] [verbose]
  user
  via
  web-cc
  xsec
```

Description

Display license usage information.

Parameter	Description
acr	Show ACR license usage
ap	Show AP license usage information.
capacity	Show capacity license usage information.
client [pool <pool>] [verbose]	Show license usage for the global configuration pool, or specify a pool name to view license usage within a specific license pool. Use the optional <code>verbose</code> parameter too display aggregated license usage for each configuration node and managed devices in those nodes.
user	Show Policy Enforcement Firewall (PEF) user license usage.
via	Show VIA license usage information.
webcc	Show WebCC license usage information.
xsec	Show Extreme Security (xSec) user and tunnel license usage.

Examples

The following example displays the user license usage.

```
(host) #show license-usage user

User License Usage
-----
Name                Value
-----
```

```

License Limit      2048
License Usage      12
License Available  2036
License Exceeded   0

```

The AP license usage is displayed below:

```

(host) #show license-usage AP

AP Licenses
-----
Type                Number
----                -
AP Licenses         48
MM Licenses         41
MC-VA Licenses      48
MC-VA country       IN
Controller License   True
Overall AP License Limit 41

AP Usage
-----
Type                Count
----                -
Active CAPs                    0
Standby CAPs [Counted Against Total] 0
Active RAPs                    0
Remote-node APs                0
Active MUX                     0
Active PUTN                    0
Total APs                      0

Remaining AP Capacity
-----
Type  Number
----  -
CAPs  509
RAPs  509

```

When you issue the `show license-usage client` command from the CLI of a controller configured as a centralized licensing server, the output displays license usage statistics for each licensing client associated to that server. Include the `verbose` parameter to display license statistics for individual configuration nodes and the devices in those nodes. The output in the example below is separated into multiple tables to better fit in this document. In the ArubaOS CLI, the output appears in a single wide table.

```

(MM) [mynode] #show license-usage client verbose
License Clients License Usage for pool /
-----

```

```

Hostname  IP Address      Mac addr          AP   PEF   RF Protect
-----
RagSC     10.15.90.33    00:0c:29:71:10:15  0   0     0
Rag-LC1   2002::3        00:1a:1e:01:b2:28  3   3     0
TOTAL     3              3                 3   3     0

ACR      WebCC   MM      MC-VA-RW  MC-VA-EG  MC-VA-IL  MC-VA-JP  MC-VA-US  VIA
-----
0        0       0       0         0         0         0         0         0
0        0       0       0         0         0         0         0         0
0        0       0       0         0         0         0         0         0

Last update (secs. ago)
16
Total no. of clients: 0

Node level usage details for pool /
-----
Node-Path  AP   PEF   RF Protect  ACR  WebCC  MM      MC-VA-RW  MC-VA-EG
MC-VA-IL  MC-VA-JP  -----
/          0   0     0           0   0     0       0         0         0
0
MC-VA-US  VIA
-----
0        0

License Clients License Usage for pool /md/hq/voip/x86
-----
Hostname  IP Address      Mac addr  AP   PEF   RF Protect  ACR  WebCC  MM
MC-VA-RW  MC-VA-
-----
-----EG  MC-VA-IL  MC-VA-JP  MC-VA-US  VIA  Last update
(secs. ago)
-----
Total no. of clients: 0

Node level usage details for pool /md/hq/voip/x86
-----
Node-Path  AP   PEF   RF Protect  ACR  WebCC  MM      MC-VA-RW  MC-VA-EG
MC-VA-IL  MC-VA-JP  -----
/          0   0     0           0   0     0       0         0         0
0
MC-VA-US  VIA
-----
0        0

```

The output of the `show license-usage client` command includes the following data columns:

Parameter	Description
Hostname	Name of the licensing client controller.
IP Address	IPv4 or IPv6 address of the licensing client controller.
AP	Total number of AP licenses used by a licensing client associated with this controller.
PEF	Total number of Policy Enforcement Firewall (PEF) licenses used by a licensing client associated with this controller.
RF Protect	Total number of RFprotect licenses used by a licensing client associated with this controller.
ACR	Total number of advanced Cryptography (ACR) licenses used by a licensing client associated with this controller.
WebCC	Total number of Web Content Classification (WebCC) licenses used by a licensing client associated with this controller.
MM	Total number of Mobility Conductor (MM) licenses used by a licensing client associated with this controller.
MC-VA-RW MC-VA-EG MC-VA-IL MC-VA-JP MC-VA-US	Total number of regional licenses required to terminate APs on a virtual controller. Different MC-VA-XX license types enable APs to support regional channels for the following countries: <ul style="list-style-type: none"> ■ MC-VA-US: United states ■ MC-VA-JP: Japan ■ MC-VA-IL: Israel ■ MC-VA-EG: Egypt ■ MC-VA-RW: Rest of the world (all other countries)
Last update (secs. ago)	Time, in seconds, that has elapsed since the licensing table on the licensing client was updated.

Related Commands

Command	Description
license	This command allows you to install, delete, and manage software licenses on Mobility Conductor.
show license aggregate	Display the total number of licenses of each license type in all Mobility Conductor licensing pools.
show license keys	Display information about all installed license keys.

Command	Description
<code>show license box</code>	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.6.0.0	The command output also displayed IPv6 address in <code>IP addressparameter</code> .
ArubaOS 8.4.0.0	The <code>Active MUX</code> and <code>Active PUTN</code> parameters were added.
ArubaOS 8.0.1.0	The <code>verbose</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Conductor.

show lldp interface

```
show lldp interface gigabitethernet <slot/module/port>
```

Description

This command displays the LLDP interfaces information.

Parameter	Description
gigabitethernet <slot/module/port>	Displays LLDP information on a gigabitethernet interface.

Example

The example shows two commands. The output of the `show lldp interface` command displays information for all LLDP interfaces.

```
(host) #show lldp interface
LLDP Interfaces Information
-----
Interface LLDP TX LLDP RX LLDP-MED TX interval Hold Timer
-----
GE1/3      Enabled Enabled Enabled 30 120
The following example only shows information for the GE1/3 interface.
(host)[node] #show lldp interface gigabitethernet 0/0/3
Interface: gigabitethernet 0/0/3
LLDP Tx: Enabled, LLDP Rx: Enabled
LLDP-MED: Enabled
Transmit interval: 30, Hold timer: 120
```

Parameter	Description
Interface	Name of an LLDP interface.
LLDP TX	Shows if LLDP Protocol Data Unit (PDU) transmission is enabled or disabled.
LLDP RX	Shows if the managed device has enabled or disabled processing of received LLDP PDUs.
LLDP-MED	Shows if LLDP MED protocol is enabled or disabled.
TX interval	The LLDP transmit interval, in seconds.
Hold Timer	The LLDP transmit hold multiplier.

Related Commands

Command	Description
ap lldp profile	Define an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

show lldp neighbor

show lldp neighbor interfaces gigabitethernet <slot/module/port> [detail]

Description

This command displays information about LLDP peers.

Parameter	Description
gigabitethernet <slot/module/port>	Displays LLDP information on a gigabitethernet interface.
detail	Include details.

Example

The command in the first example below shows that the ports GE0/0/1 and GE0/0/2 recognize each other as an LLDP peers.

```
(host)#show lldp neighbor
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-----
Local Intf Chassis ID Capability Remote Intf Expiry-Time (Secs)
-----
GE0/0/1 00:0b:86:6a:25:40 B:R GE0/0/17 105
GE0/0/2 00:0b:86:6a:25:40 B:R GE0/0/18 105
System name
-----
Aruba 7220
Aruba 7220
Number of neighbors: 2
(host) #show lldp neighbor interface gigabitethernet 0/0/3 detail
Interface: gigabitethernet 0/0/3, Number of neighbors: 1
-----
Chassis id: d8:c7:c8:ce:0d:63, Management address: 192.168.0.252
Interface description: bond0, ID: d8:c7:c8:ce:0d:63, MTU: 1522
Device MAC: d8:c7:c8:ce:0d:63
Last Update: Thu Sep 27 10:59:37 2012
Time to live: 120, Expires in: 103 Secs
System capabilities : Bridge,Access point
Enabled capabilities: Access point
System name: IAP-105
System description:
ArubaOS (MODEL: 105), Version 6.1.3.4-3.1.0.0 (35380)
Auto negotiation: Supported, Enabled
Autoneg capability:
10Base-T, HD: yes, FD: yes
100Base-T, HD: yes, FD: yes
```



```

1000Base-T, HD: no, FD: yes
Media attached unit type: 1000BaseTFD - Four-pair Category 5 UTP, full
duplex mode (30)
MAC: 7c:d1:c3:c7:e9:72: Blacklist
MAC: 9c:b7:0d:7d:0b:72: Blacklist
MAC: 7c:d1:c3:d1:02:c8: Blacklist

```

The output of the `show lldp neighbor` command includes the following information:

Parameter	Description
Local Intf	Slot and port number.
Chassis ID	MAC address of the LLDP Peer.
Capability	Shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
Remote Intf	Remote interface.
Expiry-time	Expiry time.
System Name	Name of the peer system, as supplied by the peer.

The output of the `show lldp neighbor interface gigabitethernet <slot/module/port> detail` command varies, depending upon the type of LLDP peer detected. The output in the example above contains the following information:

Parameter	Description
Interface	Name of the port for which you are viewing LLDP neighbor information.
Number of Neighbors	Number of LLDP neighbors seen by the port.
Chassis id	MAC address of the neighbor device.
Management address	MAC address of the neighbor's management port.
Interface description	Description of the LLDP neighbor interface.
ID	Interface ID of the LLDP neighbor interface.
MTU	Maximum Transmission Unit size allowed by the neighbor device in bytes.
Device MAC	Shows the MAC address of the IAP connected to the MAS port.

Parameter	Description
Last Update	Date and time the neighbor device's status changed.
Time to live	Time, in seconds, for which this information is valid.
Expires in	Time, in seconds, before this information is considered invalid.
System capabilities	This column shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
Enabled capabilities	This column if the peer has been actively configured to operate as a router, bridge, access point, phone or other network device.
System name	Name of the peer system, as supplied by the peer.
System description	Description of the peer system, as supplied by the peer.
Auto negotiation	Shows if link auto-negotiation is enabled for the peer interface.
Media attached unit type	This parameter displays additional details about an LLDP-MED device attached to the interface. The specific details depend upon the capabilities of the device.
VLAN	VLAN ID assigned to the peer interface.
pvid	Indicates if the VLAN ID is assigned to the peer access port.
MAC	Shows the MAC address of the rogue AP detected by the Instant AP(IAP), which is blacklisted by the MAS.
LLDP-MED	Shows details for LLDP-MED (Media Endpoint Discovery), if applicable.
Device Type	Type of LLDP-MED device connected to the peer interface.
Capability	Capabilities of the LLDP-MED device connected to the peer interface.

Related Commands

Command	Description
ap lldp profile	Define an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

show lldp statistics

```
show lldp statistics gigabitethernet <slot/module/port>
```

Description

This command displays the LLDP statistics information. By default, this command displays LLDP statistics for the entire list of LLDP interfaces. Include a slot/module/port number to display statistics specific to the interface.

Parameter	Description
<code>gigabitethernet <slot/module/port></code>	Displays LLDP information on a gigabitethernet interface.

Example

The example command below shows LLDP statistics for the Gigabit Ethernet interface **0/0/0**.

```
(host) #show lldp statistics interface gigabitethernet 0/0/0

LLDP Statistics
-----
Interface           Received   Unknow TLVs   Malformed   Transmitted
-----
gigabitethernet0/0  1249      0              0           1249
```

The output of this command includes the following information:

Parameter	Description
Interface	Name of an LLDP interface.
Received	Number of packets received on that interface.
Unknown TLVs	Number of LLDP Protocol Data Units (PDUs) with an unknown type-length-value (TLV).
Number of Malformed packets	Number of malformed packets received on that interface.
Transmitted	Number of packets transmitted from that interface.

Related Commands

Command	Description
ap lldp profile	Define an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

show local-cert-mac

```
show local-cert-mac
tag <mac>
```

Description

Display the IP, MAC address and certificate configuration of a managed device in a Mobility Conductor/managed device configuration. By default the output of this command shows each managed device's IP and MAC address and the type of certificate used by those managed devices (Custom or Factory). Use the optional `tag` parameter to display information for a managed device only.

Parameter	Description
<code>tag <tag></code>	IP address of the managed device or MAC address of the managed device.

Example

The output of this command shows that two managed devices have a custom certificate installed.

```
(host)[node] # show local-cert-mac
Local Switches configured by Local Certificate
-----
Switch IP of the Local  MAC address of the Local  Cert-Type  CA cert
-----
10.4.62.3                0B:86:F0:12:AC:15          Custom     CAcert
10.4.62.5                00:0B:86:F0:05:60          Custom     Undefined
```

The output of this command includes the following information:

Parameter	Description
Switch IP of the Local	IP address of the managed device.
MAC address of the Local	MAC address of a managed device with a local certificate.
Cert-Type	Type of certificate used by the local managed device. <ul style="list-style-type: none">■ Custom: User-installed, custom certificate■ Factory: Factory-installed certificate
CA Cert	Name of the Certificate Authority (CA) certificate.

Related Commands

Command	Description
local-factory-cert	This command configures the factory-installed certificate for secure communication between a managed device and Mobility Conductor.
local-custom-cert	This command configures a custom certificate for secure communication between a managed device and Mobility Conductor.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show localip

```
show localip
  tag <local-switch-ip>
```

Description

Displays the IP address and VPN shared key between master/ conductor and local.

Parameter	Description
tag <local-switch-ip>	Displays VPN configuration of a specific local switch.

Example

The output of this command shows the managed device's IP address and shared key between Mobility Conductor and managed devices.

```
(host)[node] # show localip

Local Switches configured by Local Switch IP
-----
Switch IP address of the Local  Key
-----
0.0.0.0                        *****
```

Related Commands

Command	Description
localip	This command configures the IP address and preshared key for the managed device on a Mobility Conductor.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show localipv6

show localipv6

Description

Shows the IP address and preshared key for the managed device on a Mobility Conductor.

Parameter	Description
<tag>	Show VPN configuration of a specific Local Switch or Output Modifiers.

Example

This example shows the IPv4 and IPv6 addresses configured .

```
(host) [mynode] (config) #show localipv6
Local Switches configured by Local Switch IPv6
-----
Switch IPv6 address of the Local  Corres IPv4 address of the Local  Key
-----
2002::1                          1.1.1.1                          *****
```

Related Commands

Command	Description
localipv6	This command configures the IP address and preshared key for the managed device on a Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show local-peer-mac

Syntax

```
show local-peer-mac tag <local-mac-addr>
```

Description

This command is used to display the MAC address used for secure communication based between Mobility Conductor and managed devices.

Parameter	Description
tag <local-mac-addr>	The managed device's MAC address.

Example

Include the optional tag <local-mac-addr>

```
(host) [mynode] (config) #local-peer-mac 00:0c:29:00:00:00 ipsec 123456
```

Related Commands

Command	Description
local-peer-mac	This command is used to configure security peer-mac based between Mobility Conductor and managed devices.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show local-userdb

```
show local-userdb
  maximum-expiration
  start <offset>
  page <page-size>
  username <username>
  verbose
```

Description

Shows information about user's accounts in the local user database. Issue this command without any parameters to display a general overview of user's accounts in the database. Use the `maximum-expiration` parameter to show how long the account is valid for in minutes. Use the `start <offset>`, `page <page_size>` parameters to control which user account records in the database display initially and the number of account records displayed on a page.

Parameter	Description
<code>maximum-expiration</code>	How long the account is valid, in minutes, in the internal database.
<code>start <offset></code>	Display records starting at a specific database record number defined by the <code><offset></code> parameter.
<code>page <page-size></code>	Number of user entries to display .
<code>username <username></code>	Show data for a specific user.
<code>verbose</code>	Display the following additional details for each database entry. <ul style="list-style-type: none">▪ Full-Name▪ Company▪ Phone▪ Comments▪ Start-Date▪ Creation-Date▪ Sponsor-Fullname▪ Sponsor-Email▪ Sponsor-Dept▪ Opt-Field-1▪ Opt-Field-2▪ Opt-Field-3▪ Opt-Field-4▪ Grantor-Role▪ VLAN▪ NASIP

Example

This example shows the basic summary of user accounts in the database.

```
(host)[node] #show local-userdb maximum-expiration start 5 page 4

local-userdb maximum-expiration 90

User Summary
-----
Name          Password  Role    E-Mail  Enabled  Expiry  Status  Sponsor-
Name Grantor-Name
-----
- -----
guest-0657984  *         guest   Yes     Yes      Active
admin
guest-8330301  *         guest   Yes     Yes      Active
admin
guest-5433352  *         guest   Yes     Yes      Active
admin
guest-3469360  *         guest   Yes     Yes      Active
admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the user.
Password	The user's password.
Role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
E-mail	Shows the email address of the user account.
Enabled	Shows whether the account is enabled or disabled.
Expiry	Shows the expiration date for the user account. If this is not set, the account does not expire.
Status	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Sponsor-Name	Shows the sponsor's name.

Parameter	Description
Grantor-Name	Shows the grantor's name.
User Entries	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show local-userdb-guest

```
show local-userdb-guest
  maximum-expiration
  start <offset>
  page <page-size>
  username <username>
  verbose
```

Description

Shows information about guest accounts in the local user database. Issue this command without any parameters to display a general overview of guest accounts in the database. Use the `maximum-expiration` parameter to show validity period of the account, in minutes. Use the `start <offset>`, `page <page_size>` parameters to control which guest account records in the database display initially and the number of account records displayed on a page.

Parameter	Description
<code>maximum-expiration</code>	How long the account is valid, in minutes, in the internal database.
<code>start <offset></code>	Display records starting at a specific database record number defined by the <code><offset></code> parameter.
<code>page <page-size></code>	Number of user entries to display .
<code>username <username></code>	Show data for a specific user.
<code>verbose</code>	Display the following additional details for each database entry. <ul style="list-style-type: none">▪ Full-Name▪ Company▪ Phone▪ Comments▪ Start-Date▪ Creation-Date▪ Sponsor-Fullname▪ Sponsor-Email▪ Sponsor-Dept▪ Opt-Field-1▪ Opt-Field-2▪ Opt-Field-3▪ Opt-Field-4▪ Grantor-Role▪ VLAN▪ NASIP

Example

This example shows the basic summary of guest user accounts in the database.

```
(host)[node] #show local-userdb-guest maximum-expiration start 5 page 4
local-userdb-guest maximum-expiration 90

Guest UserSummary
-----
Name          Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-
Name Grantor-Name
-----
- -----
guest-0657984  *  guest   Yes     Yes     Active
  admin
guest-8330301  *  guest   Yes     Yes     Active
  admin
guest-5433352  *  guest   Yes     Yes     Active
  admin
guest-3469360  *  guest   Yes     Yes     Active
  admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the user.
Password	The user's password.
Role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
E-mail	Shows the email address of the user account.
Enabled	Shows whether the account is enabled or disabled.
Expiry	Shows the expiration date for the user account. If this is not set, the account does not expire.
Status	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Sponsor-Name	Shows the sponsor's name.

Parameter	Description
Grantor-Name	Shows the grantor's name.
User Entries	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show local-userdb-public-access

```
show local-userdb-public-access
  maximum-expiration
  start <offset>
  page <page-size>
  username <username>
  verbose
```

Description

Shows information about public-access user accounts in the local user database. Issue this command without any parameters to display a general overview of guest accounts in the database. Use the `maximum-expiration` parameter to show how long the account is valid for in minutes. Use the `start <offset>`, `page <page_size>` parameters to control which account records in the database display initially and the number of account records displayed on a page.

Parameter	Description
<code>maximum-expiration</code>	How long the account is valid, in minutes, in the internal database.
<code>start <offset></code>	Display records starting at a specific database record number defined by the <code><offset></code> parameter.
<code>page <page-size></code>	Number of user entries to display .
<code>username <username></code>	Show data for a specific user.
<code>verbose</code>	Display the following additional details for each database entry. <ul style="list-style-type: none">▪ Full-Name▪ Company▪ Phone▪ Comments▪ Start-Date▪ Creation-Date▪ Sponsor-Fullname▪ Sponsor-Email▪ Sponsor-Dept▪ Opt-Field-1▪ Opt-Field-2▪ Opt-Field-3▪ Opt-Field-4▪ Grantor-Role▪ VLAN▪ NASIP

Example

This example shows the basic summary of public access user accounts in the database.

```
(host)[node] #show local-userdb-guest maximum-expiration start 5 page 4
local-userdb-guest maximum-expiration 90

Guest UserSummary
-----
Name          Password  Role    E-Mail  Enabled  Expiry  Status  Sponsor-
Name  Grantor-Name
-----
-
-----
guest-0657984  *         guest   Yes     Yes      Active
admin
guest-8330301  *         guest   Yes     Yes      Active
admin
guest-5433352  *         guest   Yes     Yes      Active
admin
guest-3469360  *         guest   Yes     Yes      Active
admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the user.
Password	The user's password.
Role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
E-mail	Shows the email address of the user account.
Enabled	Shows whether the account is enabled or disabled.
Expiry	Shows the expiration date for the user account. If this is not set, the account does not expire.
Status	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Sponsor-Name	Shows the sponsor's name.

Parameter	Description
Grantor-Name	Shows the grantor's name.
User Entries	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show localip

```
show localip
tag <local-switch-ip>
```

Description

Displays the IP address and VPN shared key between master/ conductor and local.

Parameter	Description
tag <local-switch-ip>	Displays VPN configuration of a specific local switch.

Example

The output of this command shows the managed device's IP address and shared key between Mobility Conductor and managed devices.

```
(host)[node] # show localip

Local Switches configured by Local Switch IP
-----
Switch IP address of the Local  Key
-----
0.0.0.0                        *****
```

Related Commands

Command	Description
localip	This command configures the IP address and preshared key for the managed device on a Mobility Conductor.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

show log

```
show log
  all
  ap-debug
  arm
  arm-user-debug
  errorlog
  network
  peer-debug
  security
  system
  user
  user-debug
  wireless [<number>]
```

Description

Show the log files on Mobility Conductor or a managed device.

Parameter	Description
all	Issue the command <code>show log all</code> to display all log files. Include this parameter after one of the log file types (for example, <code>show log security all</code>) to display all log files of the selected type.
ap-debug	Display AP debug log files.
arm	Display ARM log files.
arm-user-debug	Display ARM user debug log files.
errorlog	Display error log files.
network	Display network log files.
peer-debug	Display peer debug log files.
security	Display security log files.
system	Display system log files.
user	Display user log files.
user-debug	Display user debug log files.
wireless <number>	Display wireless log files.

Parameter	Description
	Include this parameter at the end of the show log command to start displaying the log output from the specified number of lines from the end of the log.

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.
logging-trace-files	The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show log all

```
show log all [<number>]
```

Description

Shows the log files on Mobility Conductor or a managed device.

Parameter	Description
<number>	Include this parameter at the end of the show log command to start displaying the log output from the specified number of lines from the end of the log.

Example

This example shows the log files on Mobility Conductor or a managed device.

```
(host)[mynode] #show log all
-- Generating SQL statements from diff
-----
-----
15 Oct 23:23:32 ntpd[7266]: Listen and drop on 0 v6wildcard [::]:123
15 Oct 23:23:32 ntpd[7266]: Listen and drop on 1 v4wildcard 0.0.0.0:123
15 Oct 23:23:32 ntpd[7266]: Listen normally on 2 lo 127.0.0.1:123
15 Oct 23:23:32 ntpd[7266]: Listen normally on 3 lo [::1]:123
15 Oct 23:23:32 ntpd[7266]: Listen normally on 4 eth1
[fe80::20c:29ff:fe62:5b07%6]:123
15 Oct 23:23:32 ntpd[7266]: Listening on routing socket on fd #21 for
interface updates
At Thu Oct 15 23:21:57 IST 2020 Starting DB upgrade for wms
At Thu Oct 15 23:22:08 IST 2020 Postgres DB upgrade done for wms
At Thu Oct 15 23:23:22 IST 2020 Starting DB upgrade for upgrademgrdb
At Thu Oct 15 23:23:28 IST 2020 Postgres DB upgrade done for upgrademgrdb
At Thu Oct 15 23:23:41 IST 2020 Starting DB upgrade for gapdb
At Thu Oct 15 23:23:46 IST 2020 Postgres DB upgrade done for gapdb
Comparing schema data
Creating temporary /tmp/pgdiff_gapdb folder for upgrade operations
Creating temporary /tmp/pgdiff_upgrademgrdb folder for upgrade operations
Creating temporary /tmp/pgdiff_wms folder for upgrade operations
Creating temporary DB comparisondatabase_gapdb
Creating temporary DB comparisondatabase_upgrademgrdb
Creating temporary DB comparisondatabase_wms
Creating temporary database gapdb_tmp
Creating temporary database upgrademgrdb_tmp
Creating temporary database wms_tmp
Deleting comparisondatabase_gapdb
Deleting comparisondatabase_upgrademgrdb
Deleting comparisondatabase_wms
```

```

Deleting temporary database gapdb_tmp and related /mswitch/conf/gapdb_6_1_
tmp.sql file
Deleting temporary database upgrademgrdb_tmp and related
/mswitch/conf/upgrademgr_psql_tmp.sql file
Deleting temporary database wms_tmp and related /mswitch/conf/wms_pg_schema_
tmp.sql file
ERROR: constraint "cpsec_whitelist/allowlist_pkey" of relation "cpsec_
whitelist/allowlist" does not exist
ERROR: constraint "rap_whitelist/allowlist_pkey" of relation "rap_
whitelist/allowlist" does not exist
ERROR: constraint "userinfo_pkey" of relation "userinfo" does not exist
Extracted schema data for postgresql://root@127.0.0.1:5432/gapdb
Extracted schema data for postgresql://root@127.0.0.1:5432/gapdb_tmp
Extracted schema data for postgresql://root@127.0.0.1:5432/upgrademgrdb
Extracted schema data for postgresql://root@127.0.0.1:5432/upgrademgrdb_tmp
Extracted schema data for postgresql://root@127.0.0.1:5432/wms
Extracted schema data for postgresql://root@127.0.0.1:5432/wms_tmp
Extracting schema data for gapdb
Extracting schema data for gapdb_tmp
Extracting schema data for upgrademgrdb
Extracting schema data for upgrademgrdb_tmp
Extracting schema data for wms
Extracting schema data for wms_tmp
FATAL: database "cfgmdb" does not exist
FATAL: database "root" does not exist
Fri Oct 16 00:00:41 2020, 0, 0, 0, 0, 0, 0, 0, 0
Fri Oct 16 00:01:41 2020, 0, 0, 0, 0, 0, 0, 0, 0
Fri Oct 16 00:02:42 2020, 0, 0, 0, 0, 0, 0, 0, 0
Fri Oct 16 00:03:42 2020, 0, 0, 0, 0, 0, 0, 0, 0
Fri Oct 16 00:04:42 2020, 0, 0, 0, 0, 0, 0, 0, 0
Fri Oct 16 00:05:42 2020, 0, 0, 0, 0, 0, 0, 0, 0

```

Command History

Version	Description
ArubaOS 8.9.0.0	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> All instances of <code>master</code> have been replaced with <code>conductor</code>. All instances of <code>slave</code> have been replaced with <code>member</code>. All instances of <code>blacklist</code> have been replaced with <code>denylist</code>. All instances of <code>whitelist</code> have been replaced with <code>allowlist</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show log ap-debug

```
show log ap-debug{ [<number>] [all]}
```

Description

Show the controller's AP debug logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the AP debug logs for the controller.

Example

This example shows the ten most recent AP debug logs for the controller.

```
(host)[node] #show log ap-debug 10

Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): Copyright (c) 2005-2006 Atheros
Communications, Inc. All Rights Reserved
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi0: Base BSSID
00:1a:1e:25:97:d0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi1: Base BSSID
00:1a:1e:25:97:c0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): ^H<6>Ethernet Channel Bonding
Driver: v3.0.1 (January 9, 2006)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): secure_jack_link_state_change:
Error finding device eth0
Nov 24 20:54:25  KERNEL(AP39@10.6.1.21): Kernel watchdog refresh ended.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show log arm

show log arm

Description

Show the controller's ARM logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the ARM user debug logs for the controller.

Example

This example shows the controller's ARM process log.

```
(host)[node] #show log arm all
Oct 15 23:23:38 ARM Process[6250]: <703004> <6250> <WARN> |ARM Process|
set_amon_switch_ip: changing amon switch ip addr to 10.17.24.43
Oct 15 23:23:38 ARM Process[6250]: <703004> <6250> <WARN> |ARM Process|
arm_process_service_ctrl_info_channel_events: Configured controller address
ipv6 :: ipv4 10.17.24.43 service 0.0.0.0
Oct 15 23:23:38 ARM Process[6250]: <703004> <7730> <WARN> |ARM Process|
set_amon_switch_ip: changing amon switch ip addr to 10.17.24.43
Oct 15 23:23:38 ARM Process[6250]: <703004> <7730> <WARN> |ARM Process|
arm_process_service_ctrl_info_channel_events: Configured controller address
ipv6 :: ipv4 10.17.24.43 service 0.0.0.0
Oct 15 23:23:38 ARM Process[6250]: <703004> <7730> <WARN> |ARM Process|
set_amon_switch_ip: changing amon switch ip addr to 10.17.24.43
Oct 15 23:23:38 ARM Process[6250]: <703004> <7730> <WARN> |ARM Process|
arm_process_service_ctrl_info_channel_events: Configured controller address
ipv6 :: ipv4 10.17.24.43 service 0.0.0.0
Oct 15 23:23:38 ARM Process[6250]: <703004> <7730> <WARN> |ARM Process|
set_amon_switch_ip: changing amon switch ip addr to 10.17.24.43
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show log arm-user-debug

```
show log arm-user-debug{[<number>][all]}
```

Description

Show the controller's ARM user debug logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the ARM user debug logs for the controller.

Example

This example shows the controller's last ten ARM user debug logs.

```
(host)[node] #show log arm-user-debug 10
Aug 12 16:03:03 :508164: <DEBUG> |ARM Process| Client Match: Found 11v
Capable STA b0:ee:45:49:60:3c
Aug 12 16:03:03 :508201: <DEBUG> |ARM Process| Client Match: Sending BSS
transition req to client b0:ee:45:49:60:3c token 14
Aug 12 16:03:03 :508202: <DEBUG> |ARM Process| Client Match: Timer started
for BTM response STA b0:ee:45:49:60:3c timerid 5176652
Aug 12 16:03:06 :508161: <DEBUG> |ARM Process| Client Match Received probe
report: AP 6c:f3:7f:e7:1d:20 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk
for client b0:ee:45:49:60:3c with signal -44
Aug 12 16:03:06 :508161: <DEBUG> |ARM Process| Client Match Received probe
report: AP d8:c7:c8:46:e0:00 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk
for client b0:ee:45:49:60:3c with signal -38
Aug 12 16:03:06 :508161: <DEBUG> |ARM Process| Client Match Received probe
report: AP 6c:f3:7f:e7:1d:20 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk
for client b0:ee:45:49:60:3c with signal -35
Aug 12 16:03:11 :508161: <DEBUG> |ARM Process| Client Match Received probe
report: AP d8:c7:c8:46:e0:00 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk
for client b0:ee:45:49:60:3c with signal -36
Aug 12 16:03:13 :508203: <DEBUG> |ARM Process| Client Match: Timer cleared
for BTM response STA b0:ee:45:49:60:3c timerid 5176652
Aug 12 16:03:13 :508186: <DEBUG> |ARM Process| Client Match: Tracking
unsuccessful failure for client b0:ee:45:49:60:3c num fails 0 btm rejects 0
btm timeouts 4
Aug 12 16:03:13 :508185: <DEBUG> |ARM Process| Client Match: move status:
Uncontrolled-Radio complete move for client b0:ee:45:49:60:3c from Source AP
ap135 d8:c7:c8:46:e0:00 Eff_Signal -0 dBm (Signal -0 dBm EIRP 0 dBm) to
Target AP ac 6c:f3:7f:e7:1d:20 Eff_Signal -0 dBm (Signal -0 dBm EIRP 0 dBm)
Actual AP ap135 d8:c7:c8:46:e0:00 Time diff 9 Reason Denied; User action
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show log errorlog

```
show log errorlog{[<number>][all]}
```

Description

Show the controller's system errors and other critical information.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the error logs for the controller.

Example

This example shows the ten most recent system log errors.

```
(host)[node] #show log errorlog 10
Mar 5 10:30:34 <sapd 106007> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Rogue AP detected with SSID cto-dnh-blah, BSSID
00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:31:39 <sapd 404080> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: ADHOC network detected with Src 00:13:ce:45:91:a0, BSSID
02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel 11 and RSSI 22
Mar 5 10:32:12 <sapd 106007> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Rogue AP detected with SSID cto-dnh-blah, BSSID
00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:32:46 <sapd 106007> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Rogue AP detected with SSID cto-dnh-blah, BSSID
00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:40:32 <localdb 133019> <ERRS> |localdb| User admin was not found
in the database
Mar 5 10:40:32 <localdb 133006> <ERRS> |localdb| User admin Failed
Authentication
Mar 5 10:41:10 <sapd 106007> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Rogue AP detected with SSID sw-rlo-open, BSSID
00:0b:86:c9:9e:20, Wired MAC 00:00:00:00:00:00, and IP 0.0.0.0
Mar 5 10:41:31 <sapd 106007> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Rogue AP detected with SSID QA_MARORA_VOCERA, BSSID
00:0b:86:c9:9e:21, Wired MAC 00:0b:86:02:ee:00, and IP 10.3.49.254
Mar 5 10:48:01 <sapd 404080> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: ADHOC network detected with Src 00:13:ce:45:d9:4d, BSSID
02:13:ce:28:40:48, ESSID adhoc_ap70 Channel 11 and RSSI 8
Mar 5 11:04:21 <sapd 404080> <ERRS> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: ADHOC network detected with Src 00:13:ce:45:d9:4d, BSSID
02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel 11 and RSSI 9
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show log network

```
show log network{ [<number>] [all]}
```

Description

Show the controller's system network errors.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the network logs for the controller.

Example

This example shows the controller's recent network log errors

```
(host) [node] #show log network all  
  
Feb 17 14:47:14 :209801: <WARN> |fpapps| Physical link down: port 1/1  
Feb 17 14:48:04 :209801: <WARN> |fpapps| Physical link down: port 1/1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor or managed devices.

show log peer-debug

```
show log peer-debug{[<number>] [all]}
```

Description

Show the peer-debug logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the AP debug logs for the controller.

Example

This example shows the ten most recent AP debug logs for the controller.

```
(host)[node] #show peer-debug log 10

Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): Copyright (c) 2005-2006 Atheros
Communications, Inc. All Rights Reserved
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi0: Base BSSID
00:1a:1e:25:97:d0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi1: Base BSSID
00:1a:1e:25:97:c0, 16 available BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): ^H<6>Ethernet Channel Bonding
Driver: v3.0.1 (January 9, 2006)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): secure_jack_link_state_change:
Error finding device eth0
Nov 24 20:54:25  KERNEL(AP39@10.6.1.21): Kernel watchdog refresh ended.
```

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.
logging-trace-files	The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show log security

```
show log security{[<number>][all]}
```

Description

Show the controller's security logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the security logs for the controller.

Example

This example shows the controller's last seven security logs.

```
(host)[node] #show log security 7

Mar 5 11:53:43 :124004: <DEBUG> |authmgr| Local DB auth failed for user
admin, error (User not found in UserDB)
Mar 5 11:53:43 :124003: <INFO> |authmgr| Authentication
result=Authentication failed(1), method=Management, server=Internal,
user=10.100.100.66
Mar 5 11:53:43 :124004: <DEBUG> |authmgr| Auth server 'Internal' response=1
Mar 5 11:53:43 :125027: <DEBUG> |aaa| mgmt-auth: admin, failure, , 0
Mar 5 11:53:43 :125024: <NOTI> |aaa| Authentication Succeeded for User
admin, Logged in from 10.100.100.66 port 1778, Connecting to 10.3.49.100
port 22 connection type SSH
Mar 5 11:53:58 :103060: <DEBUG> |ike| ipc.c:ipc_get_cfgm_role:2826 Sending
REQUEST for CFGM Role
Mar 5 11:53:58 :103060: <DEBUG> |ike| ipc.c:get_local_cfg_trigger_ike:2653
IKE got trigger from CFGM : state :3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor or managed devices.

show log system

```
show log system{[<number>][all]}
```

Description

Show the controller's system logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the system logs for the controller.

Example

This example shows the controller's last ten system logs.

```
(host)[node] #show log system 10

Mar 5 11:55:59 :316073: <DEBUG> |wms| Received New AP Message: AP
00:0b:86:b5:87:c2 Status 1 Num-WM 0
Mar 5 11:55:59 :316083: <DEBUG> |wms| mysql: UPDATE ap_table SET ssid='qa-
abu-customerissue', current_channel='11', type='generic-ap', ibss='no', phy_
type='80211g', rap_type='interfering', match_mac='00:00:00:00:00:00', power_
level='255', status='up' WHERE id='71575' ;
Mar 5 11:55:59 :316029: <DEBUG> |wms| Sending message to Probe:
IP:10.3.49.253 Msg-Type:PROBE_RAP_TYPE AP 00:0b:86:b5:87:c2 Type:1
Mar 5 11:55:59 :316036: <DEBUG> |wms| Received New STA Message: MAC
00:0b:86:b5:87:c2 Status 0
Mar 5 11:55:59 :316032: <DEBUG> |wms| STA Probe: ADD Probe
00:0b:86:a2:e7:40 for STA 00:0b:86:b5:87:c2
Mar 5 11:56:00 :399814: <DEBUG> |fpapps| PoE: RAN THRU ITERATION 2
Mar 5 11:56:00 :326001: <DEBUG> |AP 1.1.1@10.3.49.253 sapd| AM: am_read_
bss_data_stats: radio 0: pktsIn 0 pktsOut 0 bytesIn 0 bytesOut 0
Mar 5 11:56:00 :326001: <DEBUG> |AP 1.1.1@10.3.49.253 sapd| AM: am_read_
bss_data_stats: radio 0: pktsIn 0 pktsOut 52107 bytesIn 0 bytesOut 18143486
Mar 5 11:56:01 :326001: <DEBUG> |AP 1.1.1@10.3.49.253 sapd| AM: MPPS 2722
CPPS 338 PKTS 452036609 BYTES 2062458092 INTR 334327351
Mar 5 11:56:02 :399814: <DEBUG> |fpapps| PoE: Evaluating port 1/5 rv is 0
and crv is 1
state :3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor or managed devices.

show log user

```
show log user{[<number>][all]}
```

Description

Show the controller's user logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the user logs for the controller.

Example

This example shows the controller's last ten user logs.

```
(host)[node] #show log user 10

Mar 5 13:29:57 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:32:08 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:36:41 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:38:42 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:40:41 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:42:51 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:47:03 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:49:07 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:53:08 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:55:14 :501083: <WARN> |stm| Probe request: 00:0b:86:cd:1a:00:
Invalid Station MAC address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Conductor and managed devices.

show log user-debug

```
show log user-debug{[<number>] [all]}
```

Description

Show the controller's user debug logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the user debug logs for the controller.

Example

This example shows the controller's last ten user debug logs.

```
(host)[node] #show log user-debug 10

Mar 5 13:57:24 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:57:24 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:41-1.1.1 SSID
Mar 5 13:58:26 :501082: <DEBUG> |stm| Probe request: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:58:26 :501085: <DEBUG> |stm| Probe request: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:26 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:26 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:41-1.1.1 SSID
Mar 5 13:58:27 :501082: <DEBUG> |stm| Probe request: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:58:27 :501085: <DEBUG> |stm| Probe request: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:27 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:27 :501090: <DEBUG> |stm| Probe response: 00:18:f8:ab:77:a4: AP
10.3.49.253-00:0b:86:a2:e7:41-1.1.1 SSID
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show log wireless

```
show log wireless{[<number>][all]}
```

Description

Show the controller's wireless logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the wireless logs for the controller.

Example

This example shows the controller's last ten wireless logs.

```
(host)[node] #show log wireless 10

Mar 5 13:59:31 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID mak-cp-psk and BSSID
00:0b:86:8b:70:20
Mar 5 13:59:35 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID  and BSSID
00:0b:86:c0:06:83
Mar 5 13:59:38 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID  and BSSID
00:0b:86:c0:06:85
Mar 5 13:59:41 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID  and BSSID
00:0b:86:89:f9:42
Mar 5 13:59:41 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID QA-SANJAY-OSUWIRELESS
and BSSID 00:0b:86:89:f9:40
Mar 5 13:59:44 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID QA-SANJAY-OSUVOICE and
BSSID 00:0b:86:8c:fb:c0
Mar 5 13:59:44 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID Google and BSSID
00:0b:86:4f:82:c0
Mar 5 13:59:47 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID QA-SANJAY-OSUVOICE and
BSSID 00:0b:86:89:f9:41
Mar 5 13:59:50 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM
00:0b:86:a2:e7:40: Interfering AP detected with SSID  and BSSID
00:0b:86:c0:06:86
```

```
Mar 5 13:59:50 :404003: <WARN> |AP 1.1.1@10.3.49.253 sapd| AM  
00:0b:86:a2:e7:40: Interfering AP detected with SSID cto-dnh-blah and BSSID  
00:0b:86:60:b8:80
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show log essid-debug

```
show log essid-debug{[<number>][all]}
```

Description

Show the controller's ESSID debug logs. An Extended Service Set Identifier (ESSID) is used to identify the wireless clients and Wireless Broadband Routers in a WLAN. All wireless clients and Wireless Broadband Routers in the WLAN must use the same ESSID.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the ESSID debug logs for the controller.

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.
logging-trace-files	The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor or managed devices.

show log bssid-debug

```
show log bssid-debug{[<number>][all]}
```

Description

A Basic Service Set Identifier (BSSID) uniquely defines each wireless client and Wireless Broadband Router. This command shows the controller's BSSID debug logs.

Parameter	Description
<number>	Start displaying the log output from the specified number of lines from the end of the log.
all	Shows all the BSSID debug logs for the controller.

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.
logging-trace-files	The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show logging

```
show logging facility|server|{level [verbose]}
```

Description

The IP address of the remote logging server, as well as facility log types and their associated facility levels.

The ArubaOS logging levels follow syslog convention:

- level 7: Emergency
- level 6: Alert
- level 5: Critical
- level 4: Errors.
- level 3: Warning
- level 2: Notices
- level 1: Informational
- level 0: Debug

The default logging level is **level 1**. You can change this setting via the `logging` command.

Parameter	Description
<code>facility</code>	View the facility used when logging messages into the remote syslog server.
<code>server</code>	Show the IP address of a remote logging server.
<code>level [verbose]</code>	Show logging levels at which the messages are logged. Include the optional verbose parameter to display additional data for logging subcategories and processes.

Example

This example below displays defined logging levels for each logging facility.

```
(host)[node] #show logging level
LOGGING LEVELS
-----
Facility  Level
-----  -
network   warnings
security  warnings
system    warnings
user      warnings
```

```
wireless warnings
```

This example below displays the IP address of a remote log server. If a remote log server has not yet been defined, this command will not display any output.

```
(host)[node] #show logging server
Remote Server: 1.1.1.1

FACILITY MAPPING TABLE
-----
local-facility  severity  remote-facility
-----
user            debugging local1
```

The following example displays the status of the TLS configuration.

```
(NODE) #show logging server
Remote Server: 2.2.2.2 Destination Port: 514
FACILITY MAPPING TABLE
-----
local-facility  severity  remote-facility  CEF Format  BSD RFC 3164
Compliance     source-interface  tls option
-----
---  -----
All      Disabled      debugging local1      Disabled      Disabled
          Disabled      Enabled
```



If the destination port is not configured, the default port 514 will be used for rsyslog to establish the TCP connection. The default facility will be local1. CLI will display error messages if TLS is enabled simultaneously either with source-interface or CEF.

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, as well as facility log types and their associated facility levels.

Command History

Version	Description
ArubaOS 8.9.0.0	The output sub-parameter <code>tls</code> was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show loginsessions

show loginsessions

Description

Displays the current administrator login sessions statistics.

Example

Issue this command to display the admin login session statistics.

```
Session Table
-----
ID  User Name  User Role  Connection From  Idle Time  Session Time
--  -
1   admin     root      10.100.102.43   00:00:00  00:27:59
```

The output includes the following parameters:

Parameter	Description
ID	Sessions identification number
User Name	Administrator's user name
User Role	Administrator's role
Connection From	The IP address from which the administrator is connecting
Idle Time	Amount of time the user has been idle
Session Time	Total time the session has been open

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Configuration mode on Mobility Conductor.

show mac-address-table

show mac-address-table

Description

Displays a MAC forwarding table.

Example

Issue this command to display the MAC forwarding table.

```
Dynamic Address Count:          0
Static Address (User-defined) Count:      0
System Self Address Count:
Total MAC Addresses :          6
Maximum MAC addresses :          6
MAC Address Table
-----
Destination Address  Address Type  VLAN  Destination Port
-----
00:0b:86:00:00:00   Mgmt        1     vlan 1
00:0b:86:f0:05:60   Mgmt        1     vlan 1
00:0b:86:00:00:00   Mgmt        62    vlan 62
00:0b:86:f0:05:60   Mgmt        62    vlan 62
00:0b:86:00:00:00   Mgmt       4095   vlan 4095
00:0b:86:f0:05:60   Mgmt       4095   vlan 4095
```

The output includes the following parameters:

Parameter	Description
Dynamic Address Count	Count of dynamic addresses currently associated with the managed device.
Static Address (User-defined) Count	Count of static, user-defined addresses associated with the managed device.
System Self Address Count	Number of self system addresses.
Total MAC Addresses	Total number of MAC addresses associated with the managed device.
Maximum MAC Addresses	Maximum number of MAC addresses.
Destination Address	Destination MAC address.

Parameter	Description
Address Type	Destination address type.
VLAN	Associated VLAN.
Destination Port	Destination port.

Related Commands

Command	Description
mac-address-table	This command adds a static entry to the MAC address table.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show managed-device images

show managed-device images

Description

This command displays the images of managed devices stored in the Mobility Conductor file server.

Example

```
(host) [mynode] #show managed-device images
Flash Memory Status :
-----
Total 5918M, Used 2310M, Free 3608M
MD Images Directory Memory Status :
-----
Total 2048M, Used 809M, Free 1239M
MD Images Version Status :
-----
Total Versions 2, Versions Present 77133 77118
Managed Device Images :
-----
ArubaOS_72xx_8.8.0.0-mm-dev_77118
ArubaOS_72xx_8.8.0.0-mm-dev_77133
ArubaOS_VMC_8.8.0.0-mm-dev_77118
ArubaOS_VMC_8.8.0.0-mm-dev_77133
```

Related Commands

Command	Description
managed-device delete image	This command deletes the image stored in Mobility Conductor file system.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor and managed device.

show master-configpending/show conductor-configpending

show master-configpending/show conductor-configpending

Description

Displays the list of global commands which are not saved and are not sent to the managed device.

Example

This example below displays the commands which are not saved and are not sent to the managed device.

```
(host) #show master-configpending/show conductor-configpending
aaa profile "default-xml-api"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2" key "12345678"
aaa profile "default-xml-api"
aaa profile "default-xml-api" xml-api-server "10.17.93.2"
user-role "logon"
user-role "logon" captive-portal "default"
user-role "logon"
user-role "logon" no captive-portal "default"
user-role "logon"
user-role "logon" captive-portal "default"
voice rtp-analysis-config
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config no rtp-analysis
voice rtp-analysis-config rtp-analysis
```

Related Commands

Command	Description
master-redundancy master-vrrp/conductor-redundancy conductor-vrrp	This command associates a VRRP instance with Mobility Conductor redundancy.
masterip/conductorip	This command displays the statistics between the managed device and Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show master-local stats / show conductor-local stats

```
show master-local stats / show conductor-local stats
  ipv4-addr
  ipv6-addr
  page
```

Description

Display statistics for communication between Mobility Conductor and managed devices. By default, Mobility Conductor and managed devices exchange heartbeat messages every 10 seconds. These heartbeats include a configuration timestamp. If a Mobility Conductor has later timestamp than the managed device, the state of the managed device changes from Update Successful to Update Required.

Parameter	Description
<ipv4-addr>	Include the IPv4 address of a managed device to display statistics of that managed device only.
<ipv6-addr>	Include the IPv6 address of a managed device to display statistics of that managed device only.
<page>	Start displaying the output of this command at the specified page number.

Example

This example below shows statistics for all communications between the Mobility Conductor and the managed devices.

```
(host) [mynode] #show master-local stats / show conductor-local stats

Missed -> HB Req from Local(s)
-----
IPv4 Address IPv6 Address          HB Req HB Resp Cfg Terminate Peer Reset
Total Missed Last Sent Missed
-----
-----
None          2620:11d:6030:11c5::193 9      19      0          0
0              0
Total Switches:1
```

The output of this command includes the following data columns:

Parameter	Description
IPV4 Address	IPv4 address of the managed device.
IPV6 Address	IPv6 address of the managed device.
HB Req	Heartbeat requests sent from the managed device.
HB Resp	Heartbeat responses sent from the Mobility Conductor.
Cfg Terminate	Number of times the managed device has failed to upgrade to a new configuration.
Peer Reset	The number of times the connection to peer is been reset. The connection could reset due to network connectivity problems or when the peer switch reboots.
Total Missed	Total number of heartbeats that were not received by the managed device.
Last Sent Missed	This counter increments if the managed device misses the last heartbeat from the peer managed device. This counter keeps incrementing until the heartbeat message is received from peer.

Command History

Version	Modification
ArubaOS 8.7.0.0	The output of the command was modified to include IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show master-l3redundancy/show conductor-l3redundancy

```
show master-l3redundancy/show conductor-l3redundancy
  config-sync <status>
  status
  switches
```

Description

Displays the Layer-3 configuration and database sync status as well as the current status of Layer-3-domain Mobility Conductor redundancy.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
config-sync <status>	Displays Layer-3 configuration and database sync status.
status	Displays current status of Layer-3 domain master/conductor redundancy.
switches	Displays active and standby controllers on both Layer-3 peers.

Examples

The example below executed on the managed device displays the Layer-3 redundancy configuration.

```
(host) [mynode]#show master-l3redundancy/show conductor-l3redundancy
L3 Sync Role:Primary
L3 Redundant Peer IP:10.9.196.154
IKE PSK: 16c591a3789da6eef4420a5fe45967c3f1cf1bc457464244
```

The example below executed on the managed device displays the Layer-3 configuration and database sync status.

```
(host) [mynode] #show master-l3redundancy config-sync status/show conductor-
l3redundancy config-sync
Command applicable only on current Active of L3 Secondary

(host)[mynode]# show database synchronize
```

```
Last L2 synchronization time: Standby not synchronized since last reboot
Last L3 synchronization time: Secondary not synchronized since last reboot
L2 Periodic synchronization is disabled
L3 Periodic synchronization is disabled
Synchronization doesn't include Captive Portal Custom data
```

The example below executed on the managed device displays the health of primary and secondary data centers.

```
(host) [mynode]#show master-l3redundancy status/show conductor-l3redundancy
status
L3 Redundancy Status
-----
Role IP Address Status
----
Conductor 10.9.196.151 Down
Secondary Conductor 10.9.196.152 Up
```

The example below executed on the managed device allows the user to see the Layer-3 redundant peer controller details along with active and standby controller details:

Primary

```
(host) [mynode] #show master-l3redundancy switches/show conductor-
l3redundancy switches
L3 Redundancy Controllers
-----
IP Address IPv6 Address Name Type Managing MDs
-----
10.9.196.222 2001::222 ArubaMM-VA_C7_32_38 Primary-Active True
10.9.196.213 2001::213 ArubaMM-VA_16_CF_C8-Test Secondary-Active False
10.9.196.162 2001::1 mm2 Secondary-Standby N/A

(host) [mynode] #show switches
All Switches
-----
IP Address IPv6 Address Name Location Type Model Version Status
Configuration State Config Sync Time (sec) Config ID
-----
-----
10.9.196.222 2001::222 ArubaMM-VA_C7_32_38 Building1.floor1 master/conductor
ArubaMM-VA 8.8.0.0-mm-dev_0000 up UPDATE SUCCESSFUL 0 2
10.9.196.223 None ArubaMC-VA_BD_4E_10 Building1.floor1 MD ArubaMC-VA
8.8.0.0-mm-dev_0000 up UPDATE SUCCESSFUL 10 2
10.9.196.212 None ArubaMC-VA_BD_4C_F7 Building1.floor1 MD ArubaMC-VA
8.8.0.0-mm-dev_0000 up UPDATE SUCCESSFUL 10 2
Total Switches: 3

Secondary
(Host) [mynode] #show master-l3redundancy switches/show conductor-
l3redundancy switches
L3 Redundancy Controllers
```

```

-----
IP Address IPv6 Address Name Type Managing MDs
-----
10.9.196.213 2001::213 ArubaMM-VA_16_CF_C8-Test Secondary-Active False
10.9.196.162 2001::1 mm2 Secondary-Standby N/A
10.9.196.222 2001::222 ArubaMM-VA_C7_32_38 Primary-Active True

(Host) [mynode] #show switches
All Switches
-----
IP Address IPv6 Address Name Location Type Model Version Status
Configuration State Config Sync Time (sec) Config ID
-----
-----
10.9.196.213 2001::213 ArubaMM-VA_16_CF_C8-Test Building1.floor1
master/conductor ArubaMM-VA 8.8.0.0-mm-dev_0000 up UPDATE SUCCESSFUL 0 23
10.9.196.162 2001::1 mm2 Building1.floor1 standby ArubaMM-VA 8.8.0.0-mm-dev_
0000 up UPDATE SUCCESSFUL 0 23
Total Switches: 2

```

Related Commands

Command	Description
master-l3redundancy/conductor-l3redundancy	This command configures Layer-3 redundancy for a Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.8.0.0	Command modified to allow users to see the Layer-3 redundant peer controller details along with active and standby controller details.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on managed device.

show master-redundancy/show conductor-redundancy

show master-redundancy/show conductor-redundancy

Description

Display the Mobility Conductor's redundancy configuration.

Example

This example below shows the current master/conductor redundancy configuration, including the ID number of the master VRRP virtual router and the IP address of the peer managed device for master/conductor redundancy.

```
(host) [mynode] (config) #show master-redundancy/show conductor-redundancy
Master/Conductor redundancy configuration:
  VRRP Id 120 current state is MASTER
  Peer's IP Address is 10.17.65.117
  Peer's IPSEC Key is *****
```

Related Commands

Command	Description
master-redundancy master-vrrp/conductor-redundancy conductor-vrrp	This command associates a VRRP instance with Mobility Conductor redundancy.
vrrp	This command configures the VRRP.
master-redundancy peer-ip-address/conductor-redundancy peer-ip-address	This command configures the IP address and preshared key or certificate for a redundant Mobility Conductor on another Mobility Conductor.

Command History

Version	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show memory

```
show memory
aaa
amon_recvr
amon_sender
ap {ble_daemon|lldpd|meshd|ofald|rapper|rfd|sapd|stm|wcd}
  {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
apimagemgr
apprf
arci-cli-helper
arm
aruba-central
as_visibility
auth
ble_daemon_s
ble_relay
blmgr
certmgr
cfgdist
cfgm
cli
cluster_mgr
cluster_upgrade_mgr
cpsec
ctamon
ctrlmgmt
dbsync
dds
debug
dhcpd
dhcpdwrap
dot1x1
dpagent
ecc
fpapps
fw_visibility
gsmmgr
ha_mgr
im_helper
ip_flow_export
isakmpd
l2tpd
lagm
licensemgr
lldpd
mdns
mobileip
mon_serv
mon_serv_fwv
nbapi
ofa
off-loader
ospf
```

pdm
 phonehome
 pim
 pptpd
 profmgr
 rtpa
 slb
 snmpd
 stm
 syslogdwrap
 tm
 tunneled_node_mgr
 ucm
 udbserver
 upgrademgr
 user_visibility
 vrrp
 web_cc
 wms
 wpa3_sae

Description

This command displays the used and available memory on Mobility Conductor. Include a process name to display a memory information for a process on the AP or Mobility Conductor.

Use this command under the supervision of Aruba technical support to help debug process errors. Include the name of a process to show memory information for that process.

The optional output modifiers `| begin` , `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
aaa	Displays memory information for the AAA process.
amon_recvr	Displays the memory information for the amon_recvr process.
amon_sender	Displays the memory information for the amon_sender process
ap	Displays memory information for a process running on a specific AP or BSSID. <ul style="list-style-type: none"> ▪ ble_daemon: Displays the memory information for the ble_daemon process. ▪ lldpd: Displays the memory information for the LLDP process. ▪ meshd: Displays the memory information for the meshd process.

Parameter	Description
	<ul style="list-style-type: none"> ▪ ofald: Displays the memory information for the OpenFlow Agent Lite Daemon process. ▪ raper: Displays the memory information for the rapper process. ▪ rfd: Displays the memory information for the rfd process. ▪ sapd: Displays the memory information for the sapd process. ▪ stm: Displays the memory information for the AP stm process. ▪ wcd: Displays the memory information for the AP wcd process.
apimagemgr	Displays the memory information for the apiimagemgr process.
apprf	Displays the memory information for the AppRF process.
arcli-helper	Displays the memory information for the aruba-central process.
arm	Displays the memory information for the ARM process.
aruba-central	Displays the memory information for the ARM process.
as_visibility	Displays the memory information of Air Slice visibility process.
auth	Displays the memory information for the authentication process.
ble_daemon_s	Displays the memory information for the ble-daemon process on the controller..
ble_relay	Displays the memory information for the ble relay process.
blmgr	Displays the memory information for the blmgr process.
certmgr	Displays the memory information for the certmgr process.
cfgdist	Displays the memory information for the cfgdist process.
cfgm	Displays the memory information for the cfgm process.
cli	Displays the memory information for the cli process.
cluster_mgr	Displays the memory information for the cluster_mgr process.

Parameter	Description
cluster_upgrade_mgr	Displays the memory information for the cluster_upgrade_mgr process.
cpsec	Displays the memory information for the cpsec process.
ctamon	Displays the memory information for the ctamon process.
ctrlmgmt	Displays the memory information for the ctrlmgmt process.
dbsync	Displays the memory information for the dbsync process.
dds	Displays the memory information for dds process.
debug	Displays detailed memory information to debug memory errors.
dhcpcd	Displays the memory information for the DHCP process.
dhcpcdwrap	Displays the memory information for the dhcpcdwrap process.
dot1x1	Displays the memory information for the dot1x1 process.
dpagent	Displays the memory information for the DPagent process.
ecc	Displays the DRAM ecc counters.
fpapps	Displays the memory information for the fpapps process.
fw_visibility	Displays the memory information for the fw_visibility process.
gsmmgr	Displays the memory information for gthe smmgr process.
ha_mgr	Displays the memory information for the HA_MGR process.
im_helper	Displays the memory information for the im_helper process.
ip_flow_export	Displays the memory information for the ip flow export process.
isakmpd	Displays the memory information for the isakmpd process.
l2tpd	Displays the memory information for the l2tpd process.
lagm	Displays the memory information for the lagm process.
licensemgr	Displays the memory information for the licensemgr process.
lldpd	Displays the memory information for the lldpd process.
mdns	Displays the memory information for the mDNS process.

Parameter	Description
mobileip	Displays the memory information for the mobileip process.
mon_serv	Displays the memory information for the mon_serv process.
mon_serv_fwv	Displays the memory information for the mon_serv_fwv process.
nbapi	Displays the memory information for the nbapi process.
ofa	Displays the memory information for the OpenFlow Agent process.
off-loader	Displays the memory information for the off-loader process.
ospf	Displays the memory information for the OSPF process.
pdm	Displays the memory information for the Policy Domain Manager process.
phonehome	Displays the memory information for the phonehome process.
pim	Displays the memory information for the pim process.
pptpd	Displays the memory information for the pptpd process.
profmgr	Displays the memory information for the profmgr process.
rtpa	Displays the memory information for the rtpa process.
sdwan	Displays the memory information for the sdwan process.
slb	Displays the memory information for the slb process.
snmpd	Displays the memory information for the snmpd process.
stm	Displays the memory information for the stm process.
syslogdwrap	Displays the memory information for the syslogdwrap process.
tm	Displays the memory information for the telemetry manager process.
tunneled_node_mgr	Displays the memory information for the tunneled_node_mgr process.
ucm	Displays the memory information for the UCM process.
udbserver	Displays the memory information for the udbserver process.

Parameter	Description
upgrademgr	Displays the memory information for the upgrademgr process.
user_visibility	Displays the memory information for the user_visibility process.
vrrp	Displays the memory information for the vrrp process.
web_cc	Displays the memory information for the WebCC process.
wms	Displays the memory information for the WMS process.
wpa3_sae	Displays the memory information for the wpa3_sae process.

Example

The command `show memory` displays, in Kilobytes, the total memory on Mobility Conductor, the amount of memory currently being used, and the amount of free memory.

```
(host) [mynode] #show memory

Memory (Kb): total: 256128, used: 162757, free: 93371
```

Include the name of a process to show memory statistics for that process. The example below shows memory statistics for **mobileip**.

```
(host) [mynode] #show memory mobileip

Type          Num Allocs      Size Allocs      Peak Allocs      Peak Size
-----
default              1947            336545            2027            336698

PC
----
Allocs      Size
-----
0x7f6eba49f06b      2            1136
0x7f6eba4b71f2     545            8065
0x7f6eba4d239c      1              20
0x7f6eba4d3556      1              33
0x7f6eba7c5c78      2             640
0x7f6eba9fc057      1            1968
0x7f6eba9fcc1d      1           66160
0x7f6ebb515ac6      1            4816
0x7f6ebc0492d6     585           32760
0x7f6ebc049ec5     543           30408
0x7f6ebc04a6e0      5             280
0x7f6ebc04bae2     36            3744
0x7f6ebc04bb05     36           14704
0x7f6ebc04bd4e     51            1224
0x7f6ebc04be5e      9             288
```

0x7f6ebc054e3e	22	528
0x7f6ebc0555be	12	480
0x7f6ebc28838d	1	120
0x7f6ebc289b1d	15	1320
0x7f6ebc289cfe	1	1176
0x7f6ebc28aaff	5	440
0x7f6ebc28b654	1	88
0x7f6ebc28b667	1	8192
0x7f6ebca7755a	5	120
0x7f6ebca78679	2	16
0x7f6ebcc8d462	15	660
0x7f6ebcc8d4a2	1	88
0x7f6ebcc941d8	1	6448
0x7f6ebcc946fa	1	41000
0x7f6ebcc94717	1	41000
0x7f6ebcc94baf	1	11263
0x7f6ebcc98ec3	3	14696
0x7f6ebcc9a49f	1	16
0x4137b6	1	64
0x41bdfb	1	41000
0x435200	1	88
0x4358ac	2	272
0x4369f1	3	120
0x436a64	9	288
0x437f3a	3	168
0x45ba3a	3	72
0x45c277	4	288
total		336545
336698		

The output of this command includes the following columns:

Column	Description
Type	The <code>show memory</code> command only shows information for predefined processes, so this column always displays the parameter <code>default</code> .
Num Alloc	Current number of memory allocations.
Size Allocs	Total size of all memory allocations, in bytes.
Peak Allocs	Maximum number of allocations used throughout in the life of the process.
Peak Size	Maximum size of allocations used throughout in the life of the process, in bytes.
PC	Program counter (PC) is the address of a memory allocation. (For internal use only)

Column	Description
Allocs	Number of memory allocations at that program counter. (For internal use only)
Size	Size of all memory allocations at that program counter. (For internal use only)

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>tm</code> parameter was added.
ArubaOS 8.7.0.0	The <code>as_visibility</code> parameter was added.
ArubaOS 8.5.0.0	The <code>wcd</code> sub-parameter was added.
ArubaOS 8.2.0.0	The <code>lagm</code> and <code>vrrp</code> parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show mgmt-role

show mgmt-role

Description

This command allows the user to view a list of management role configurations.

Example

Issue this command to display a list of management user roles.

```
Management User Roles
-----
ROLE                DESCRIPTION
----                -
root                Super user role
read-only           Read only commands
network-operations network-operations
guest-provisioning guest-provisioning
location-api-mgmt   location-api-mgmt
no-access           Default role, no commands are accessible for this role
location-api-mgmt   location-api-mgmt
```

The output includes the following parameters:

Parameter	Description
Role	Name of the management user role
Description	Description of the management user role

Related Commands

Command	Description
mgmt-user	This command configures an administrative user.
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show mgmt-server

```
show mgmt-server
  message-counters process {arm|auth|dhcp|fpapps|fw_
  visibility|hwmon|mdns|resolver|spectrum stm|tm|ucm|wms}
  profile <profile-name>
```

Description

Displays the message counter information of management server.

Parameter	Description
message-counters	Message counter in the recent past.
process {arm auth dhcp fw_visibility mdns resolver spectrum stm tm ucm wms}	controller processes: <ul style="list-style-type: none">■ arm: Advanced Radio Management (ARM)■ auth: Authentication■ dhcp: DHCP■ fpapps: Layer 2,3 control■ fw_visibility: Firewall Visibility■ hwmon: Hardware monitor■ mdns: AirGroup■ resolver: Resolver■ spectrum: Spectrum Analysis■ stm: Station Management■ tm: Telemetry Manager■ ucm: Unified Communication Manager■ wms: WLAN Management System
profile <profile-name>	Displays the list of configuration profiles and the details of the specified configuration profiles for the management server.

Example

The output of this command shows the message counter information of the WLAN Management System process in the controller.

```
(host)[node] (config) #show mgmt-server message-counters process wms
Message Counter History
-----
Message Number  Time                               Packets  Monitored AP Info
Monitored AP Stats  Monitored STA Info  Monitored STA Stats
-----  -----  -----  -----
-----  -----  -----  -----
```

82		Tue Apr 2 14:56:43 2013	1	0	0
	3		3		
81		Tue Apr 2 14:56:13 2013	1	14	218
	2		67		
80		Tue Apr 2 14:55:43 2013	1	0	0
	0		2		
79		Tue Apr 2 14:55:13 2013	1	0	0
	0		2		

The output of the following command displays the details of the default-amp management configuration profile:

```
(host)[node] #show mgmt-server profile default-amp
Mgmt Config profile "default-amp" (Predefined (editable))
-----
Parameter      Value
-----
Stats           Enabled
Tag             Enabled
Sessions        Enabled
Monitored Info  Disabled
Monitored Stats Disabled
Misc            Enabled
Location        Enabled
Voice Info      Disabled
```

Related Commands

Command	Description
mgmt-user	This command configures an administrative user.
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The tm process was added.
ArubaOS 8.2.0.0	The fpapps and hwmon parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show mgmt-servers

show mgmt-servers

Description

Displays list of management servers that receive Advanced Monitoring (AMON) messages from the controller.

Parameter	Description
mgmt-servers	Management Servers. This could be AirWave Management Server or any other server that receive messages from the controller using AMON protocol.

Example

The output of this command shows list of management servers.

```
(host) (mynode) #show mgmt-servers
List of Management Servers
-----
Primary Server  Profile      Transport-method
-----
2001::2        default-amp  secure-udp
40.40.40.1     default-amp  secure-udp
10.1.1.11      default-amp  udp
20.16.11.1     default-ale  udp
Num Rows:4
Starting from ArubaOS 8.9.0.0, the output of this command is modified as follows:
(host) (mynode) #show mgmt-servers
List of Management Servers
-----
Primary Server  Profile      Transport-method  Server Status
-----
10.9.217.71    default-controller  udp               conductor
Num Rows:1
```

Related Commands

Command	Description
mgmt-user	This command configures an administrative user.
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.1.0.0	Listed primary servers with IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mgmt-user

```
show mgmt-user <username>
  audit-info <username>
  console <username>
  local-authentication-mode <username>
  ssh-pubkey <username>
  webui-cacert <username>
  <username>
```

Description

Displays the list of management users on the controller and the details of each management user.

Parameter	Description
audit-info	Displays the audit information related to a specified management user.
console	Displays the serial console status of a management user.
local-authentication-mode	Displays the status of the local-authentication mode.
ssh-pubkey	Displays the number of management users using the ssh-pubkey.
webui-cacert	Displays the number of management users using web CA certificates.
username	Displays the details of a specified management user. Starting from ArubaOS 8.10.0.0, the range of characters in the username is increased from 1-64 to 1-128.

Example

The output of this command shows the client certificate name, username, user role, and revocation checkpoint for management users using the ssh-pubkey in the controller.

```
#show mgmt-user ssh-pubkey

SSH Public Key Management User Table
-----
CLIENT-CERT          USER          ROLE          STATUS          REVOCATION
CHECKPOINT Max-concurrent-sessions
-----          ----          ----          -----          -----
-----          -----
```

```
pub1          public1      root          ACTIVE      none
  N/A
master-ssh-pub-cert  seamless-logon  read-only    ACTIVE      none
  32
```

The output of this command displays the maximum number of concurrent sessions for a management user.

```
(host) [mynode] #show mgmt-user <username>
Management User Table
-----
USER      PASSWD  ROLE    STATUS  PATH  Max-concurrent-sessions
-----
admin     ***** root    ACTIVE  /      N/A
luke      ***** root    ACTIVE  /      N/A
```

Related Commands

Command	Description
mgmt-user	This command configures an administrative user.
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.10.0.0	The range of characters in the username is increased from 1-64 to 1-128.
ArubaOS 8.4.0.0	The following parameters were introduced: <ul style="list-style-type: none"> audit-info console The <code>max-concurrent-sessions</code> parameter was introduced in the output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show mobility-managers

show mobility-managers

Description

Use the command to display information for MMS server.

Example

Execute the following command to display the MMS information:

```
(host) [mm] (config) #show mobility-managers
MMS SERVERS
-----
HOST      USER NAME  PORT  INTERVAL  RETRY  RTLS-PORT  ACTIVE
-----
1.1.1.1   testUN     162   60         3      8000
MMS config sync state: Ready
Last Cfg sync result:  None
Automatic config update: Disabled
MMS config ID:         0
Controller config ID:  0
Config update success: 0
Config update failures: 0
```

Related Commands

Command	Description
mobility-manager	This command configures the mobility manager server for the managed device to communicate with it.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show mon-serv

```
show mon-serv
  ap-microboot-stats
  device-count
  function-stats
  max-q-stats
  message-stats
  mon-device-operation-stats
  queue-stats
  radio-microboot-stats
  sta-microboot-stats
  vap-microboot-stats
```

Description

This command shows the detailed statistics of monitoring server.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
<u>ap-microboot-stats</u>	Displays the AP micro-bootstrapping statistics.
<u>device-count</u>	Displays the count of devices that are added or deleted.
<u>function-stats</u>	Displays the summary of monitoring server activities.
<u>max-q-stats</u>	Displays the details of maximum queue statistics.
<u>message-stats</u>	Displays the AMON and monitoring server message statistics.
<u>mon-device-operation-stats</u>	Displays the device operation statistics.
<u>queue-stats</u>	Displays the current queue statistics.
<u>radio-microboot-stats</u>	Displays the micro-bootstrapping statistics of AP radios.
<u>sta-microboot-stats</u>	Displays the STA micro-bootstrapping statistics.
<u>vap-microboot-stats</u>	Displays the VAP micro-bootstrapping statistics.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv ap-microboot-stats

show mon-serv ap-microboot-stats

Description

This command displays the AP micro-bootstrapping statistics.

Example

The following example displays the AP micro-bootstrapping statistics.

```
(host) [mynode] #show mon-serv ap-microboot-stats
ENTRY MISSING (STATS) 0
ENTRY (WAIT STATE) 0
ENTRY (WAIT TO READY STATE) 0
ENTRY (READY STATE) 0
ENTRY (CREATED BY AMON) 0
ENTRY (CREATED BY BOOTSTRAP) 0
ENTRY (CREATED BY MICROBOOT) 0
ENTRY (PARENT MISSING) 0
ENTRY (PARENT IN WAIT STATE) 0
ENTRY (PARENT IN READY STATE) 0
ENTRY (PARENT UNKNOWN) 0
ENTRY (DELETED IN WAIT STATE) 0
ENTRY (DELETED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST CREATED) 0
ENTRY (WITH CHILD WAITLIST REMOVED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST REMOVED IN WAIT STATE) 0
ENTRY (MICROBOOT REQUEST SENT) 0
ENTRY (MICROBOOT REQUEST RECVD) 0
ENTRY (MICROBOOT REQUEST RECVD FOR DELETED ENTRY) 0
ENTRY (DELETED BY CLEANUP) 0
ENTRY (DELETED BY AGING) 0
ENTRY (DELETED BY AMON) 0
ENTRY (DELETED BY MON) 0
ENTRY (EXTRA INFO RACE CONDN) 0
ENTRY (LIST INSERT FAILED) 0
ENTRY (LIST REMOVE FAILED) 0
ENTRY (PARENT MISSING IN BULK BOOTSTRAP) 0
ENTRY (MULTIPLE MICROBOOT RESPONSE RECVD) 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv device-count

show mon-serv device-count

Description

This command displays a count of devices that are added or deleted.

Example

The following example shows a count of devices that are added or deleted.

```
(host) [mynode] #show mon-serv device-count
Num Ap Added                0
Num Ap Deleted              0
Num Ap Xml Req              0
Num Radio Added             0
Num Radio Deleted           0
Num Radio Xml Req           0
Num Vap Added               0
Num Vap Deleted             0
Num Vap Xml Req             0
Num Sta Added               59
Num Sta Deleted             89
Num Sta Xml Req             0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv function-stats

```
show mon-serv function-stats
```

Description

This command displays the summary of monitoring server activities.

Example

The following example shows the summary of monitoring server activities.

```
(host) [mynode] ##show mon-serv function-stats
-----
Mon stats summary
-----
Add Counts
dev_add_count          252
dev_add_bulk_count     0
rel_add_count          0
dev_add_child_count    0
-----
Delete Counts
dev_del_count          0
dev_del_mc_count       161
dev_del_all_count      0
dev_del_all_mc_count   0
rel_del_count          0
rel_del_mc_count       0
dev_del_bulk_count     0
dev_del_bulk_mc_count  0
-----
Update Counts
dev_update_info_count  233188
dev_update_stats_count 0
dev_update_stats_mc_count 70507
rel_update_info_count : 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv max-q-stats

show mon-serv max-q-stats

Description

This command shows the details of maximum queue statistics.

Example

The following example shows the details of maximum queue statistics.

```
(host) [mynode] #show mon-serv max-q-stats
Max Cumulative Mon Queue Statistics
-----
MaxQ Limit Exceeded Count          0
Max Queue Size                     0
Max size measured at: Thu Jan  1 05:30:00 1970
=====
====
Config params:
RHS Q proc lag threshold time      = 120 seconds
Punish duration for RHS Q lag      = 300 seconds
Punish duration if local Q full    = 10 seconds
Max retries if local Q full        = 10 (catnap time 100 ms)
=====
====
AMON pkt ACL statistics:
Local Q: retry incidents           0, avg retries    0
=====
====
=====
====
RHS Queue   : enqueued      310006 dequeued      310006 hi-wmark    35
length      0
RHS Queue   : Lagging behind by 0 seconds, 0 updates pending
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv message-stats

show mon-serv message-stats

Description

This command displays the AMON and monitoring server message statistics.

Example

The following example shows the AMON and monitoring server message statistics.

```
(host) [mynode] #show mon-serv message-stats
-----
Message type 0 number: 10687
Message type 1 number: 53440
Message type 2 number: 116
Message type 3 number: 0
Message type 4 number: 0
Message type 5 number: 0
Message type 6 number: 0
Message type 7 number: 0
Message type 8 number: 0
Message type 9 number: 0
Message type 10 number: 135
Message type 11 number: 1066
Message type 12 number: 7
Message type 13 number: 0
Message type 14 number: 0
Message type 15 number: 0
Message type 16 number: 0
Message type 17 number: 0
Message type 18 number: 0
Message type 19 number: 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv mon-device-operation-stats

```
show mon-serv mon-device-operation-stats
```

Description

This command shows the the device operation statistics.

Example

The following example shows the device operation statistics on the monitoring server.

```
(host) [mynode] #show mon-serv mon-device-operation-stats

Device Type: 0 [MON_DEVICE_TYPE_NETWORK]

Add Count          : 7
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 0

Device Type: 1 [MON_DEVICE_TYPE_NETWORK_FWV]

Add Count          : 0
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 0

Device Type: 2 [MON_DEVICE_TYPE_AP]

Add Count          : 316
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 3 [MON_DEVICE_TYPE_RADIO]

Add Count          : 1615
Delete Count       : 1615
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 4 [MON_DEVICE_TYPE_STA]

Add Count          : 138
Delete Count       : 157
Add Bulk Count     : 0
Delete Bulk Count  : 0
```

```
Delete All Count : 909

Device Type: 5 [MON_DEVICE_TYPE_USER]

Add Count      : 205
Delete Count   : 36
Add Bulk Count : 0
Delete Bulk Count : 0
Delete All Count : 909

Device Type: 6 [MON_DEVICE_TYPE_SSID]

Add Count      : 0
Delete Count   : 0
Add Bulk Count : 0
Delete Bulk Count : 0
Delete All Count : 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv queue-stats

show mon-serv queue-stats

Description

This command shows the current queue statistics.

Example

The following example shows the current queue statistics.

```
(host) [mynode] #show mon-serv queue-stats
Update Queue: enqueued      310364 dequeued      310364 hi-wmark      35
length      0
Query Queue : enqueued      2536 dequeued      2536 hi-wmark      3
length      0
Event Queue : enqueued      0 dequeued      0 hi-wmark      0
length      0
-----
Update Queue: Lagging behind by 0 seconds, 0 updates pending
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv radio-microboot-stats

```
show mon-serv radio-microboot-stats
```

Description

This command shows the micro-bootstrapping statistics of AP radios.

Example

The following example shows the micro-bootstrapping statistics of AP radios.

```
(host) [mynode] #show mon-serv radio-microboot-stats
ENTRY MISSING (STATS)                                0
ENTRY (WAIT STATE)                                   0
ENTRY (WAIT TO READY STATE)                          0
ENTRY (READY STATE)                                  0
ENTRY (CREATED BY AMON)                              0
ENTRY (CREATED BY BOOTSTRAP)                         2
ENTRY (CREATED BY MICROBOOT)                        0
ENTRY (PARENT MISSING)                              0
ENTRY (PARENT IN WAIT STATE)                        0
ENTRY (PARENT IN READY STATE)                       0
ENTRY (PARENT UNKNOWN)                              0
ENTRY (DELETED IN WAIT STATE)                       0
ENTRY (DELETED IN READY STATE)                      0
ENTRY (WITH CHILD WAITLIST CREATED)                 0
ENTRY (WITH CHILD WAITLIST REMOVED IN READY STATE)  0
ENTRY (WITH CHILD WAITLIST REMOVED IN WAIT STATE)   0
ENTRY (MICROBOOT REQUEST SENT)                     0
ENTRY (MICROBOOT REQUEST RECVD)                    0
ENTRY (MICROBOOT REQUEST RECVD FOR DELETED ENTRY)   0
ENTRY (DELETED BY CLEANUP)                          0
ENTRY (DELETED BY AGING)                            0
ENTRY (DELETED BY AMON)                             0
ENTRY (DELETED BY MON)                              0
ENTRY (EXTRA INFO RACE CONDN)                       0
ENTRY (LIST INSERT FAILED)                          0
ENTRY (LIST REMOVE FAILED)                          0
ENTRY (PARENT MISSING IN BULK BOOTSTRAP)            0
ENTRY (MULTIPLE MICROBOOT RESPONSE RECVD)          0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv sta-microboot-stats

```
show mon-serv sta-microboot-stats
```

Description

This command shows the STA micro-bootstrapping statistics.

Example

The following example shows the STA micro-bootstrapping statistics.

```
(host) [mynode] #show mon-serv sta-microboot-stats
ENTRY MISSING (STATS) 1
ENTRY (WAIT STATE) 0
ENTRY (WAIT TO READY STATE) 0
ENTRY (READY STATE) 61
ENTRY (CREATED BY AMON) 60
ENTRY (CREATED BY BOOTSTRAP) 0
ENTRY (CREATED BY MICROBOOT) 0
ENTRY (PARENT MISSING) 0
ENTRY (PARENT IN WAIT STATE) 0
ENTRY (PARENT IN READY STATE) 61
ENTRY (PARENT UNKNOWN) 0
ENTRY (DELETED IN WAIT STATE) 0
ENTRY (DELETED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST CREATED) 1
ENTRY (WITH CHILD WAITLIST REMOVED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST REMOVED IN WAIT STATE) 0
ENTRY (MICROBOOT REQUEST SENT) 0
ENTRY (MICROBOOT REQUEST RECVD) 1
ENTRY (MICROBOOT REQUEST RECVD FOR DELETED ENTRY) 0
ENTRY (DELETED BY CLEANUP) 0
ENTRY (DELETED BY AGING) 0
ENTRY (DELETED BY AMON) 59
ENTRY (DELETED BY MON) 0
ENTRY (EXTRA INFO RACE CONDN) 0
ENTRY (LIST INSERT FAILED) 0
ENTRY (LIST REMOVE FAILED) 0
ENTRY (PARENT MISSING IN BULK BOOTSTRAP) 0
ENTRY (MULTIPLE MICROBOOT RESPONSE RECVD) 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv vap-microboot-stats

show mon-serv vap-microboot-stats

Description

This command shows the VAP micro-bootstrapping statistics.

Example

The following example shows the VAP micro-bootstrapping statistics.

```
(host) [mynode]#show mon-serv vap-microboot-stats
ENTRY MISSING (STATS) 0
ENTRY (WAIT STATE) 0
ENTRY (WAIT TO READY STATE) 0
ENTRY (READY STATE) 0
ENTRY (CREATED BY AMON) 0
ENTRY (CREATED BY BOOTSTRAP) 10
ENTRY (CREATED BY MICROBOOT) 0
ENTRY (PARENT MISSING) 0
ENTRY (PARENT IN WAIT STATE) 0
ENTRY (PARENT IN READY STATE) 0
ENTRY (PARENT UNKNOWN) 0
ENTRY (DELETED IN WAIT STATE) 0
ENTRY (DELETED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST CREATED) 0
ENTRY (WITH CHILD WAITLIST REMOVED IN READY STATE) 0
ENTRY (WITH CHILD WAITLIST REMOVED IN WAIT STATE) 0
ENTRY (MICROBOOT REQUEST SENT) 0
ENTRY (MICROBOOT REQUEST RECVD) 0
ENTRY (MICROBOOT REQUEST RECVD FOR DELETED ENTRY) 0
ENTRY (DELETED BY CLEANUP) 0
ENTRY (DELETED BY AGING) 0
ENTRY (DELETED BY AMON) 0
ENTRY (DELETED BY MON) 0
ENTRY (EXTRA INFO RACE CONDN) 0
ENTRY (LIST INSERT FAILED) 0
ENTRY (LIST REMOVE FAILED) 0
ENTRY (PARENT MISSING IN BULK BOOTSTRAP) 0
ENTRY (MULTIPLE MICROBOOT RESPONSE RECVD) 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv-global-hash-tbl

```
show mon-serv-global-hash-tbl
  ap { counts | entries }
  mesh-table { counts | entries }
  vap { counts | entries }
```

Description

This command displays the global hash table entries of the monitoring server.

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
<code>ap</code>	Displays the global AP hash table.
<code>mesh-table</code>	Displays the global mesh hash table.
<code>vap</code>	Displays the global VAP hash table.
<code>counts</code>	Displays the counts of entries in global hash table of the managed device.
<code>entries</code>	Displays the global hash table entries. Use this parameter only for the purpose of debugging.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv-fwv-lc-table

```
show mon-serv-fwv-lc-table
  airgroup
  bootstrap-stats <ip-addr>
```

Description

This command shows the status of local controllers and AirGroup counters on the monitoring server.

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
<code>airgroup</code>	Displays the AirGroup counters.
<code>bootstrap-stats <ip-addr></code>	Displays the bootstrapping statistics.

Example

The following example shows the counter statistics on the controller.

```
(host) [mynode] #show mon-serv-fwv-lc-table airgroup

MON_SERV Airgroup Table
-----
LC IP          Servers  Users  Server Usage  User Usage  Server Ip Entries
User Ip Entries  Ag sessions  Mode
-----
-----
10.15.20.40  0         1      1364          1          1365          2
                0
10.15.20.41  5         0       4             0           4             0
                0
10.15.20.24  5         3       4             3           5             4
                0
Total        10        4      1372          4          1374
```

Related Commands

Command	Description
mon-serv-toggle-amon-traffic-filter	This command enables AMON traffic filter.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv-lc-table

```
show mon-serv-lc-table
  bootstrap-stats <ip-addr>
  debug
  dev-del-stats <ip-addr>
  microboot-stats <ip-addr>
```

Description

This command shows the status and counters of monitoring server.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
bootstrap-stats <ip-addr>	Shows bootstrap statistics for an lc-cluster.
debug	Shows the debug LC controller.
dev-del-stats <ip-addr>	Shows (STM) device delete reason statistics for an lc-cluster.
microboot-stats <ip-addr>	Shows micro-bootstrapping statistics and threshold counts for an lc-cluster.

Example

The following example shows the configuration status of all branch config groups on the controller.

```
(host) [mynode] #show mon-serv-lc-table airgroup
MON_SERV Local Controllers Table
-----
LC IP          BootStrap Status  AP Count Up  AP Count Down  Radio Count  VAP
Count  User Count
-----  -----
-----
10.17.24.22    SUCCESS           1             0               2             10
0
Total:         1                 1             0               2             10
0
```

Related Commands

Command	Description
mon-serv-toggle-amon-traffic-filter	This command enables AMON traffic filter.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>dev-del-stats</code> and <code>microboot-stats</code> parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show mon-serv-mesh-tbl-entry

```
show mon-serv-mesh-tbl-entry <dev-key> 2G | 5Gall | 5Glower | 5Gmiddle | 5Gupper |
6G | 60G [child-list]
```

Description

This command displays the mesh table entries of the monitoring server.

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Parameter	Description
<code>dev-key</code>	The MAC address of the AP.
<code>2G</code>	Displays the entries of 2 GHz radio band.
<code>5Gall</code>	Displays the entries of 5 GHz radio band.
<code>5Glower</code>	Displays the entries of lower 5 GHz radio band.
<code>5Gmiddle</code>	Displays the entries of middle 5 GHz radio band.

Parameter	Description
5Gupper	Displays the entries of higher 5 GHz radio band.
6G	Displays the entries of 6 GHz radio band.
60G	Displays the entries of 60 GHz radio band.
child-list	If you include this optional parameter, the output of this command will include the mesh table entries of the child node.

Command History

Release	Modification
ArubaOS 8.10.0.0	The 6G parameter was introduced.
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show neighbor devices

```
show neighbor devices
  cdp-statistics
  interface
```

Description

Show neighbor device information.

Parameter	Description
cdp-statistics	Displays CDP RX statistics.
interface	Displays neighbor information on the interface.

Example

The command in the first example below shows that the managed device recognizes two neighbor devices.

```
[host] (node) # show neighbor devices
Interface objtype is 7
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone,
(S)Station
(r)Repeater, (O)Other
Neighbor Devices Information
-----
Local Intf      Chassis ID          Capability  Remote Intf  Expiry-Time (Secs)
System
-----
-----
0/0/1           00:0b:86:6a:25:40   B:R        0/0/17       105           Aruba 7220
0/0/2           00:0b:86:6a:25:40   B:R        0/0/18       105           Aruba 7220
```

Parameter	Description
Local Intf	Slot and port number of the local interface that detected the neighbor devices.
Chassis ID	MAC address of the neighbor device.
Capability	Shows the capabilities of the neighbor device to operate as a router, bridge, access point, phone or other network device.
Remote Intf	Slot and port number of the remote interface on the neighbor device

Parameter	Description
Expiry-time	Expiry time.
System Name	Name of the neighbor device, as supplied by the neighbor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on managed devices. This command is not supported on Mobility Conductor.

show netdestination

```
show netdestination {ipv4 | ipv6 | <netdestination name>} [verbose]
```

Description

Displays IPv4 and IPv6 network destination information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
ipv4	Displays IPv4 network destinations.
ipv6	Displays IPv6 network destinations.
<netdestination name>	Displays the name or IP addresses.
verbose	Prints the netdestination table entries.

Example

Issue this command to display all netdestination configured on this managed device. The output below displays information for all configured IPv4 and IPv6 netdestinations. To display additional detailed information for an individual netdestinations, include the name of the netdestination at the end of the command.

```
(host) [mynode] #show netdestination
Name: sep23-ipv4
Destination ID: 34
Position  Type  IP addr  Mask-Len/Range
-----  ---  -
1         host  1.1.1.1  32
2         name  0.0.0.8  google.com
```

The output includes the following parameters:

Parameter	Description
Name	Network destination name.
Destination ID	Network destination ID.
Position	Network destination position.

Parameter	Description
Type	Network destination type.
IP_addr	IP address of the network destination.
Mask-Len/Range	Network destination subnet mask and range. If the netdestination object has a defined domain or host name, that value will appear in the mask-Len or Range column.

Related commands

Command	Description
netdestination	This command configures an alias for an IPv4 network host, subnetwork, or range of addresses.
netdestination6	This command configures an alias for an IPv6 network host, subnetwork, or range of addresses.

Command History

Version	Modification
ArubaOS 8.2.1.0	The <code>Destination ID</code> parameter was added to the output.
ArubaOS 8.2.0.0	The <code>ipv4</code> and <code>ipv6</code> parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	You must have a PEFNG license to configure or view a netdestination.	Enable or Config mode on Mobility Conductor.

show netexthdr

show netexthdr <alias-name>

Description

This command displays the IPv6 extension header (EH) types that are denied.

Parameter	Description
<alias-name>	Specify the EH alias name.

Example

The following command displays the denied extended header types in the default EH:

```
(host)[mynode] #show netexthdr default
Extended Header type(s) Denied
-----
51,
```

Related Commands

Command	Description
netexthdr	This command allows you to edit the packet filter options in the extension header (EH).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show netservice

```
show netservice [<string>]
```

Description

Show network services.

Issue this command without the optional `<string>` parameter to view a complete table of network services on the controller. Include the `<string>` parameter to display settings for a single network service only.

Parameter	Description
<code><string></code>	Name of a network service.

Example

The following example shows the protocol type, ports and application-level gateway (ALG) for the DHCP service.

```
(host)[mynode] #show netservice svc-dhcp
Services
-----
Name      Protocol  Ports  ALG  TYPE
----      -
svc-dhcp  udp       67-68  dhcp
```

Related Commands

Command	Description
netservice	This command configures an alias for network protocols.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp

```
show ntp
  authentication-keys
  events                NTP clock transition information
  peer                  NTP Peer Info
  servers               NTP Server Info
  status                NTP Information
  trusted-keys
```

Description

Shows NTP related information.

Parameter	Description
authentication	Displays the NTP authentication key information.
events	Displays the NTP clock transition information.
peer	Displays the NTP peer information.
servers	Displays the NTP server information.
status	Displays the NTP status information.
trusted-keys	Displays the NTP trusted keys information.

Related Commands

Command	Description
ntp	Helps configure NTP authentication keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp authentication-keys

```
show ntp authentication-keys
```

Description

Show information for the NTP authentication key.

The following example shows values for the NTP authentication keys—Key ID, Key Type, and the Secret.

```
(host) [mynode] # show ntp authentication-keys
Key Id Key Type Secret
-----
41      sha1      *****
```

The output of this command includes the following parameters:

Parameter	Description
Key ID	The key identifier used when you configured the NTP authentication key.
Key Type	The key type that you used when you configured the NTP authentication key—md5 or sha1.
Secret	The key value for the MD5/SHA1 hash used when you configured the NTP authentication key.

Related Commands

Command	Description
ntp	Helps configure NTP authentication keys.

Command History

Release	Modification
ArubaOS 8.2.1.0	The output was modified to show the SHA1 key type and secret (in encoded format), when SHA1 authentication is configured.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp events

show ntp events

Description

Shows NTP clock transition information.

Example

The following example displays the output of the `show ntp events` command.

```
(host)[mynode] #show ntp events

Mon, Oct 19 2020 10:26:07.495 System clock "Mon, Oct 19 2020
02:18:46.786803" stepped by server "192.168.215.1"
Mon, Oct 19 2020 10:35:21.345281 System running in free mode using clock
synchronized earlier from unreachable server "192.168.215.1"
Mon, Oct 19 2020 10:42:47.288 System clock "Mon, Oct 19 2020
10:35:21.345281" stepped by server "192.168.215.215"
Mon, Oct 19 2020 10:55:23.65823 System clock synchronized to new NTP server,
old "192.168.215.215", new "192.168.215.1"
Mon, Oct 19 2020 11:16:24.832222 System clock synchronized to new NTP
server, old "192.168.215.1", new "192.168.215.215"
Mon, Oct 19 2020 11:32:46.212006 System clock synchronized to new NTP
server, old "192.168.215.215", new "192.168.215.1"
Tue, Oct 20 2020 09:06:34.700682 System clock synchronized to new NTP
server, old "192.168.215.1", new "192.168.215.215"
Tue, Oct 20 2020 12:53:13.732769 System clock synchronized to new NTP
server, old "192.168.215.215", new "192.168.215.1"
Tue, Oct 20 2020 20:00:49.557954 System clock synchronized to new NTP
server, old "192.168.215.1", new "192.168.215.215"
```

Related Commands

Command	Description
ntp	Helps configure NTP authentication keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp peer

```
show ntp peer <fqdn/ip/ip6 Address>
```

Description

Show NTP peer information.

The `show ntp peer` command is used for NTP server troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the [show ntp servers](#) command to view basic settings for currently configured NTP servers.

Parameter	Description
fqdn	Fully Qualified Domain Name of NTP Server.
ip	IPv4 address of NTP Server.
ip6	Pv6 address of NTP Server.

Example

The output of this commands shows IPv4 and IPv6 address of the peer.

```
(host)[mynode]#show ntp peer 2008::2
remote 2008::2, local 2008::1
hmode client, pmode sym_active, stratum 16, precision -20
leap 11, refid [73.78.73.84], rootdistance 0.00000, rootdispersion 0.00262
ppoll 6, hpoll 6, keyid 0, version 4, association 53202
reach 000, unreach 1, flash 0x1620, boffset 0.00000, ttl/mode 0
timer 0s, flags config, bclient
reference time:      00000000.00000000  Wed, Feb  6 2036 22:28:16.000
originate timestamp: 00000000.00000000  Wed, Feb  6 2036 22:28:16.000
receive timestamp:   d6186e9b.5723196a  Sun, Oct 27 2013 21:03:23.340
transmit timestamp:  d6186e9b.5723196a  Sun, Oct 27 2013 21:03:23.340
filter delay:  0.00000  0.00000  0.00000  0.00000
0.00000  0.00000  0.00000  0.00000
filter offset: 0.000000 0.000000 0.000000 0.000000
0.000000 0.000000 0.000000 0.000000
filter order:  0      1      2      3
4      5      6      7
offset 0.000000, delay 0.00000, error bound 3.99217, filter error 0.00000
remote host:      2008::2
local interface:  2008::1
time last received:  59s
time until next send: 5s
reachability change: 61s
packets sent:      1
packets received:  1
bad authentication: 0
```

```

bogus origin:      0
duplicate:         0
bad dispersion:    1
bad reference time: 0
candidate order:   0
flags:            config, bclient

(host)[mynode]#show ntp peer 10.20.22.17

remote ::, local ::
hmode client, pmode unspec, stratum 3, precision -23
leap 00, refid [125.62.193.121], rootdistance 0.32069, rootdispersion
0.15305
ppoll 6, hpoll 6, keyid 0, version 4, association 26134
reach 001, unreachable 2, flash 0x0400, boffset 0.00113, ttl/mode 0
timer 0s, flags config, bclient
reference time:      d6186d7e.c99ed7ba  Sun, Oct 27 2013 20:58:38.787
originate timestamp: 00000000.00000000  Wed, Feb  6 2036 22:28:16.000
receive timestamp:   d6186e24.f02d3f57  Sun, Oct 27 2013 21:01:24.938
transmit timestamp:  d6186e24.f02d3f57  Sun, Oct 27 2013 21:01:24.938
filter delay: 0.00113  0.00000  0.00000  0.00000
0.00000  0.00000  0.00000  0.00000
filter offset: 0.398620  0.000000  0.000000  0.000000
0.000000  0.000000  0.000000  0.000000
filter order:  0      1      2      3
4      5      6      7
offset 0.398620, delay 0.00113, error bound 2.81735, filter error 0.00276
remote host:      10.20.22.17
local interface:  10.16.32.90
time last received: 1s
time until next send: 1s
reachability change: 1s
packets sent:     2
packets received: 1
bad authentication: 0
bogus origin:     0
duplicate:        0
bad dispersion:   0
bad reference time: 0
candidate order:   0
flags:            config, bclient, iburst

```

Related Commands

Command	Description
ntp	This command configures a Network Time Protocol (NTP) server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show ntp servers

show ntp servers [brief]

Description

Show information for Network Time Protocol (NTP) servers.

Parameter	Description
brief	Display the IP address of the defined NTP servers, iburst and key settings.

Examples

The following example shows values for the primary and backup NTP servers. The primary server is marked with an asterisk (*) and the backup server is marked with an equals sign (=). Note that a backup server will not display delay, offset or dispersion data, as it is not currently in use.

```
(host) (config) #show ntp server
NTP Server Table Entries
-----
Flags:      * Selected for synchronization
+ Included in the final selection set
# Selected for synchronization but distance exceeds maximum
- Discarded by the clustering algorithm
= mode is client
remote                local      st    poll  reach  delay
offset      disp
=====
*2012::d63d:7eff:fe46:7309    2012::40      3 1024    377    0.00169
-0.001367    0.13815
```

The output of this command includes the following parameters:

Parameter	Description
flags	The flags indicate the status of the server.
remote	IP address of the remote NTP server defined using the CLI command ntp .
local	IP address of the local clock.

Parameter	Description
st	NTP uses hierarchical levels of clock sources, or strata, and assigns each layer a number starting with zero at the root. The st column in the output of this command represents the number of servers between the configured NTP server and the root reference clock.
poll	Interval, in seconds, between the local NTP server's attempt to poll the remote NTP server.
reach	An index that measures whether or not the remote NTP server could be reached at eight most recent polling intervals. If the NTP server has just been configured and hasn't yet been polled successfully, the value will be zero (0). A value of 377 indicates that the last eight poll queries were successful.
delay	Delay, in seconds, between the time that the local clock polls the NTP server and the NTP server returns a reply.
offset	The difference in time, in seconds, between the local clock and the NTP server.
disp	Dispersion represents the maximum error of the local clock relative to the reference clock, and is a measurement of the time server and network quality. Lower dispersion values are preferred over higher dispersion values.

The following example shows the **ntp servers** configuration. The NTP server IP address, key ID and iburst status are shown when the `ntp servers brief` command is used.

The following output is for IPv4:

```
(host) (config) #show ntp servers brief
server 1.1.1.1 key 1234
server 10.1.1.245 iburst key 12345
```

The following output is for IPv6:

```
(host) (config) #show ntp servers brief
server 2012::d63d:7eff:fe46:7309
```

Related Commands

Command	Description
ntp	This command configures an NTP server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp status

show ntp status

Description

Show information for a NTP server.

Example

The following example shows values for the primary NTP server.

```
(host) #show ntp status

Authentication:          enabled
time since restart:     2347
time since reset:       7594
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0
bad length or format:   0
bad authentication:     0
rate exceeded:          0
system peer:            10.1.1.250
system peer mode:       client
leap indicator:         00
stratum:                3
precision:              -18
root distance:          0.03236 s
root dispersion:        0.06728 s
reference ID:           [10.1.1.250]
reference time:         cd45b701.bcbc05d5 Tue, Feb 17 2009 14:21:53.737
system flags:           auth monitor ntp kernel stats
jitter:                 0.005020 s
stability:              0.866 ppm
broadcastdelay:         0.003998 s
authdelay:              0.000000 s
```

The output of this command includes the following parameters:

Parameter	Description
authentication	Indicates if authentication is enabled for the NTP server.
time since restart	Time in hours since the system was last rebooted.

Parameter	Description
time since reset	The number of seconds since the last time the local NTP server was restarted.
packets received	Total number of packets received.
packets processed	Number of packets received in response to previous packets sent.
current version	Number of packets matching the current NTP version.
previous version	Number of packets matching the previous NTP version.
declined	Number of packets declined.
access denied	Number of packets for which access has been denied.
bad length or format	Number of packets with invalid length, format or port number.
packets received	Total number of packets received.
bad authentication	Number of NTP packets that failed to be authenticated.
rate exceeded	Number of packets discarded due to rate limitation.
system peer	The IP address of the peer NTP server.
system peer mode	The peer mode of this remote association: <ul style="list-style-type: none"> ▪ Symmetric Active ▪ Symmetric Passive ▪ Client ▪ Server ▪ Broadcast
leap indicator	This parameter indicates whether or not a leap-second should be inserted or removed at the end of the last day of the current month. <ul style="list-style-type: none"> ▪ 00 no warning ▪ 01 +1 second (following minute has 61 seconds) ▪ 10 -1 second (following minute has 59 seconds)
stratum	The stratum level of the peer
precision	The advertised precision of the switch. This value can range from -4 and -20, inclusive.
root distance	Total round trip delay to the stratum 1 reference clock.

Parameter	Description
root dispersion	Total dispersion to the stratum 1 reference clock. This value is a cumulative measure of all errors associated with the network hops and servers between the NTP server and its stratum 1 server.
reference ID	IPv4/IPv6 address of the remote NTP server. NOTE: When NTP server is reachable through IPv4 address, use the address as is. If done through IPv6 address, the Reference ID is calculated instead of directly taking the IPV6 address on the NTP Server. The controller performs a MD5 checksum and the last 4 bytes are considered as the reference ID.
reference time	Time when the local system clock was last set or corrected, in NTP timestamp format.
system flags	This parameter displays any flags configured for this NTP entity.
jitter	The average magnitude of jitter between several time queries.
stability	The average magnitude of offset between several time queries
broadcastdelay	The broadcast delay of this NTP server association, in seconds.
authdelay	The authentication delay of this NTP server association, in seconds.

Related Commands

Command	Description
ntp	This command configures an NTP server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ntp trusted-keys

show ntp trusted-keys

Description

Shows NTP trusted key information.

Related Commands

Command	Description
ntp	Helps configure NTP authentication keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show netstat

```
show netstat
ip dst|src <ip-addr>
port dst|exclude|src <port>
raw
stats
tcp
udp
unix
```

Description

Show network statistics for current active network connections, filtered by protocol type.

Issue the `show netstat stats` command to display aggregate statistics, or protocol type, port or IP address to filter the statistics displayed in the output of this command.

Parameter	Description
<code>ip dst src <ip-addr></code>	Displays network statistics filtered based on the source or destination IP address
<code>port dst exclude src <port></code>	Displays network statistics filtered based on the source or destination port number. Use the <code>exclude</code> parameter to exclude a part from the output of this command.
<code>raw</code>	Show netstat raw socket statistics
<code>stats</code>	Show a network statistics summary
<code>tcp</code>	Displays network statistics for TCP sockets.
<code>udp</code>	Displays network statistics for UDP sockets.
<code>unix</code>	Displays network statistics for UNIX sockets.

Example

The following example shows incoming and outgoing packet statistics for the controller.

```
(host)[node](config) #show netstat stats
Total: 1128 (kernel 1200)
TCP: 147 (estab 82, closed 22, orphaned 0, synrecv 0, timewait 13/0),
ports 0
Transport Total IP IPv6
* 1200 - -
RAW 1 1 0
UDP 240 43 197
```

TCP	125	107	18
INET	366	151	215
FRAG	0	0	0

Related Commands

Parameter	Description
netservice	Configures an alias for network protocols.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode.

show off-loader bss-info

```
show off-loader bss-info
```

Description

This command shows the current WPA3 BSS information of the Off-Loader daemon process.

Example

```
(host) [md] #show off-loader bss-info

Off-Loader BSS Information
-----
BSS                AP-Name                ESSID  Type  Supported DH Groups  GTK
IGTK
```

```

---
-----
-----
94:b4:0f:63:06:60 bc:9f:e4:ca:b1:ad OTH -- --
--
94:b4:0f:63:06:70 bc:9f:e4:ca:b1:ad OTH -- --
--
bc:9f:e4:2b:1a:d0 wli-555 OTH -- --
--
bc:9f:e4:2b:1a:e0 wli-555 OTH -- --
--

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on managed devices.

show off-loader pmk-info

```
show off-loader pmk-info
```

Description

This command shows the current WPA3 PMK information of the Off-Loader daemon process.

Example

```

(host) [md] #show off-loader pmk-info

Off-Loader PMK Information
-----
KEY  MAC  BSS  PMKID  TYPE
---  ---  ---  -----  ---

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on managed devices.

show off-loader statistics

show off-loader statistics

Description

This command shows the current operational statistical counters of the Off-Loader daemon process.

Example

The following command shows the current operational statistical counters of the Off-Loader daemon process,

```
(host) [md] #show off-loader statistics
Off-Loader Work Factory Information
-----
#Workers  Reqt Queue Size  #PMK-Cache (OWE/SAE)  #BSS (OWE/SAE)
-----
10         0 (8192)         0 (0/0)                0 (0/0)
Crypto Off-Loader Usage
-----
D-H Group  Total Usage  OWE Usage  SAE-Commit Usage  SAE-Confirm Usage
-----
19         0           0           0                   0
OWE Handling Statistics Information
-----
Req-NoPMKSA  Req-PMKSA  Resp-DH (PMK-NotMatch)  Resp-PMKSA  Resp-GrpNotSupp
Resp-BssNotSupp  Resp-Failure
-----
0           0           0 (0)                0           0
0           0
SAE Commit Request Handling Statistics Information
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on managed devices.

show openflow

```
show openflow
  capabilities
  controller
  debug
  flow-table
  flows
  ports
  statistics
```

Description

The command displays the information such as flows, flow tables, system capabilities, and statistics related to OpenFlow on the managed device where OpenFlow is enabled.

Parameter	Description
capabilities	Displays the OpenFlow system capability information.
controller	Displays the OpenFlow Controller information.
debug {ap-client event flows ports}	Displays the debug information for the OpenFlow AP clients, events, flows and ports.
flow-table	Displays the flow table information.
flows	Displays the flow information of the OpenFlow agent.
ports	Displays all the ports configured for OpenFlow.
statistics	Displays the OpenFlow statistics information.

Example

The following command displays the OpenFlow capabilities on the managed device:

```
(host-md) #show openflow capabilities

Match Fields:
In Port
Ethernet Destination Address
Ethernet Source Address
Ethernet Frame Type
802.1Q Vlan ID
IP Protocol
IPv4 Source Address
IPv4 Destination Address
TCP Source Port
```

```

TCP Destination Port
UDP Source Port
UDP Destination Port
IPv6 Source Address
IPv6 Destination Address
Actions:
Output to Port
Set 802.1Q Vlan ID
Set 802.1Q Vlan Priority
Strip 802.1Q Vlan
Set Ethernet Source Address
Set Ethernet Destination Address
Set IPv4 Source Address
Set IPv4 Destination Address
Set DSCP Bits
Set TCP/UDP Source Port
Set TCP/UDP Destination Port

```

The following command displays the OpenFlow Controller information from the managed device:

```

(host-md) #show openflow controller

Controller IP Address: 10.4.131.169  Port: 6633
Connection: UP
State: ACTIVE
Local IP: 10.4.135.67
Local Port: 39703
Last Connected: Tue Jun 21 15:33:45 2016 (83618 seconds ago)
Datapath ID: 00:00:00:0b:86:bb:cd:27
Auxiliary Channel Status:On, Last Connected: Tue Jun 21 15:35:15 2016
Total Flow Count: 25
Total Port Count: 12
Total Packet In Count: 3650
Total Packet In Count (no match): 2
Total Packet Out Count: 7859

```

The following command displays the ports configured for OpenFlow:

```

(host-md) #show openflow ports

Total number of ports: 12

Openflow Port Table
-----
Name                Port No  Mac Address          Status
-----
spiCA890700in      3        00:00:00:00:00:00    UP
bss6cf37fe97b70    9        6c:f3:7f:e9:7b:70    UP
spi03EE4D00out     1        00:00:00:00:00:00    UP
bss6cf37fe97b60    10       6c:f3:7f:e9:7b:60    UP
bssaca31effb820    12       ac:a3:1e:ff:b8:20    UP
GE0/0/2            4        00:0b:86:bb:cd:2a    UP

```

```

bssaca31eebc6c0 8      ac:a3:1e:eb:c6:c0 UP
bssaca31effb830 11     ac:a3:1e:ff:b8:30 UP
bssaca31eebc6d0 7      ac:a3:1e:eb:c6:d0 UP
bssaca31effcdf0 5      ac:a3:1e:ff:cd:f0 UP
bssaca31effcde0 6      ac:a3:1e:ff:cd:e0 UP
GE0/0/0         2      00:0b:86:bb:cd:28 UP

```

The following command displays the OpenFlow statistics:

```

(host-md) #show openflow statistics
Openflow Message Statistics
-----
Statistics-Name      Received  Sent
-----
Hello                1         1
Echo Request         0        2724
Echo Reply           2724      0
Features Request     2         0
Features Reply       0         2
Set Config           1         0
Packet In            0        3774
Port Status          0         56
Packet Out           8111      0
Flow Mod             26        0
Desc Request         1         0
Desc Reply           0         1
Flow Stats Request  2877      0
Flow Stats Reply     0        2877
Port Stats Request  1439      0
Port Stats Reply     0        1439
Port Desc Stats Request 1         0
Port Desc Stats Reply 0         1
Sos Action Add       25        25
Sos OF Enable        0         1
Sos Session Add      0         1
Sos Packet-In       3537      0
Mark Sweep Start    0         1
Mark Sweep Finished 1         0
Packet Out Local    0         11
Aux Setup            0         2
Aux Setup Retry     0         4
Aux Destroy          0         2
Aux Ready            2         0
Aux Health Chceck   8601     8601
Aux Port Map         0         15
Aux Probe            0         14
Tunnel Ipsec Update 50         0
Auth Flow Add       25        25
Auth Init            0         1
Auth Up              1         0
Auth Wired Trusted   9         0

```

Miscellaneous Counters

Counter-Name	Value
-----	-----
Ip Flow Stats Update	2459
Gsm Port Add Enqueue	296
Gsm User Add Enqueue	228
Gsm Port Add Dequeue	296
Gsm User Add Dequeue	228

The following command displays the OpenFlow flows:

```
(host-md) #show openflow flows

flow cookie 281474976710733
priority 32768
match:
Ethernet Type:IPv4
source IPv4 address: 192.168.61.3
destination IPv4 address: 192.168.60.60
ip proto: udp
dest tcp/udp port: 5003
actions:
output interfaces:65530
output interfaces:65533
IP ToS:2e,
set vlan pcp:6,
matched:0packets, 0bytes
Hard Timeout:60

Total number of flows: 27

flow cookie 281474976710734
priority 32768
match:
Ethernet Type:IPv4
source IPv4 address: 192.168.60.60
destination IPv4 address: 192.168.61.3
ip proto: udp
dest tcp/udp port: 5003
actions:
output interfaces:65530
output interfaces:65533
IP ToS:2e,
set vlan pcp:6,
matched:0packets, 0bytes
Hard Timeout:60
```

The following command displays the output of flow-table on the managed device with a Sample bi-directional flow installed by the OpenFlow Controller:

```
(host-md) #show openflow flow-table
Openflow Flow Table
-----
```

In Port	Src Mac	Dst Mac	Ether	Src IP	Dst IP	Proto
Src Port	Dst Port	Packets	Bytes	Actions		
-----	-----	-----	-----	-----	-----	-----
*	*	*	0x800	*	*	17
*	5000	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
*	5060	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
*	5002	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
*	2000	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
*	32512	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
*	1720	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
*	5060	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
*	5061	0	0	(Output:normal)		
*	*	*	0x800	1.1.1.1	2.2.2.2	97
*	*	1324	76792	(Output:controller)		
*	*	*	0x800	*	*	17
*	5070-6070	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
*	1718-1719	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
1718-1719	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
5070-6070	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	222.173.190.239	186.173.202.254	17
60000	60000	0	0	(Output:controller)		
*	*	*	0x806	*	*	*
*	*	2226	4558848	(Output:normal)	(Output:controller)	
*	*	*	0x800	192.168.61.3	192.168.60.60	17
*	5003	0	0	(Output:normal)	(Output:controller),	
(Set IP ToS:46), (Set Vlan pcp:6)						
*	*	*	0x800	192.168.60.60	192.168.61.3	17
*	5003	0	0	(Output:normal)	(Output:controller),	
(Set IP ToS:46), (Set Vlan pcp:6)						
*	*	*	0x800	*	*	6
5061	*	0	0	(Output:normal)		
*	*	*	0x800	*	*	6
1720	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
2000	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x86dd	::/0	::/0	58
136	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
5060	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
5002	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	17
5000	*	0	0	(Output:normal)	(Output:controller)	
*	*	*	0x800	*	*	6
5060	*	0	0	(Output:normal)	(Output:controller)	

```

*          *          *          0x86dd  ::/0          ::/0          58
135      *          *          0          0          (Output:normal) (Output:controller)
*          *          *          0x800  *          *          17
32512    *          *          0          0          (Output:normal) (Output:controller)
Total number of flows: 27

```

The following command displays the debug event listing the flow addition on the managed device:

```

(host-md) #show openflow debug event

Printing events sorted by time (Max 1000), Total:115
-----
114. Wed Jun 22 15:38:09 2016 : SOS ACTIONS RESP : trans_id:27, sos action_
index: 27, ethtype:2048 sipv4:192.168.60.60 dipv4:192.168.61.3 proto:17
sport:0 dport:5003
113. Wed Jun 22 15:38:09 2016 : FLOW ADD : ethtype:2048 inport:0
srcmac:00:00:00:00:00:00 dstmac:00:00:00:00:00:00 sipv6::: sipv6:::
sipv4:192.168.60.60 dipv4:192.168.61.3 proto:17 sport:0
dport:5003,idletmo:0, metadata:0, act=[ (Output:normal) (Output:controller),
(Set IP ToS:46), (Set Vlan pcp:6) ]
112. Wed Jun 22 15:38:09 2016 : SOS ACTIONS RESP : trans_id:26, sos action_
index: 26, ethtype:2048 sipv4:192.168.61.3 dipv4:192.168.60.60 proto:17
sport:0 dport:5003
111. Wed Jun 22 15:38:09 2016 : FLOW ADD : ethtype:2048 inport:0
srcmac:00:00:00:00:00:00 dstmac:00:00:00:00:00:00 sipv6::: sipv6:::
sipv4:192.168.61.3 dipv4:192.168.60.60 proto:17 sport:0
dport:5003,idletmo:0, metadata:0, act=[ (Output:normal) (Output:controller),
(Set IP ToS:46), (Set Vlan pcp:6) ]
110. Wed Jun 22 15:24:33 2016 : PORT DEL : name:spi5371BD00in, dp_
port:65553, ofp_port:14
109. Wed Jun 22 15:24:33 2016 : PORT DEL : name:spiFD0D7900out, dp_
port:65554, ofp_port:13

```

Related Commands

Command	Description
openflow-profile	This command configures OpenFlow profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on managed device.

show openflow-controller

```
show openflow-controller
  applications
  flow-table [app-name|dpid|sorted-by-dpid]
  flows [app-name <name>|dpid <dp-id>]|flow-cookie|flow-id
  forwarding-db [mac-address <mac-address>]
  hosts [dpid <dp-id>|ip-address <ip>|mac-address <mac>]
  links [dpid <dp-id>]
  ports [dpid <dp-id>]
  resource
  statistics [process-name <name>]
  summary [dpid <dp-id>]
  switches [details]
```

Description

The command displays the OpenFlow Controller configuration information on . In addition, you can view information such as flows, flow tables, hosts, and statistics related to OpenFlow Controller on Mobility Conductor.

Parameter	Description
applications	Displays the application information.
flow-table [app-name dpid sorted-by-dpid]	Displays the flow table information on Mobility Conductor. You can also filter the view based on the application name that installed the flow, or by datapath ID of the OpenFlow instance.
flows [app-name <name> dpid <dp-id>]	Displays the flow information of the OpenFlow Controller on Mobility Conductor.
forwarding-db	Displays data per client for the forwarding database.
hosts [dpid <dp-id> ip-address <ip> mac-address <mac>]	Displays the OpenFlow host configuration information on Mobility Conductor. You can also filter the view by datapath ID, IP address or MAC address of the host.

Parameter	Description
links [dpid <dp-id>]	Displays the OpenFlow links on Mobility Conductor. You can also filter the output based on the datapath ID of the OpenFlow instance.
ports [dpid <dp-id>]	Displays the OpenFlow ports configured on Mobility Conductor. You can also filter the output based datapath ID of the OpenFlow instance.
resource	Displays the OpenFlow resource usage information on Mobility Conductor.
statistics [process-name <name>]	Displays the OpenFlow statistics information. You can also filter the output based on any of the following process names: <ul style="list-style-type: none"> ■ flow_manager ■ topology ■ topology_discovery ■ routing_switch ■ switch_manager ■ packetin_dispatcher ■ event_dispatcher
summary [dpid <dp-id>]	Displays the OpenFlow summary information on Mobility Conductor. You can also filter the output based datapath ID of the OpenFlow instance.
switches [details]	Displays the details of the OpenFlow switches on Mobility Conductor.

Example

The following command displays the OpenFlow Controller configuration details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller
openflow-controller
-----
Parameter          Value      Set
-----          -
ofc state           Enabled
```

```
ofc host-ageout-time      300
ofc mode                  passive
ofc certificate-file      none
ofc key-file              none
ofc ca-certificate-file   none
ofc tls                   Disabled
ofc port                  6633
ofc topology-discovery    Disabled
ofc auxiliary-channel-port 6633
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller applications

show openflow-controller applications

Description

Displays the application information.

Example

The following command displays the OpenFlow Controller applications details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller applications
Applications
-----
Name      Status   Type
----      -
AirGroup  Enabled  External
ucm       Enabled  External
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller flow-table

```
show openflow-controller flow-table
  app-name
  dpid
  sorted-by-dpid
```

Description

The command displays the flow table information on Mobility Conductor. You can also filter the view based on the application name that installed the flow, or by datapath ID of the OpenFlow instance.

Parameter	Description
app-name	Displays the name of app that installed the flow.
dpid	The dpid of the switch.
sorted-by-dpid	List of applications sorted by dpid.

Example

The following command displays the flow table information for the routing_switch app:

```
(host) [mynode] #show openflow-controller flow-table app-name routing_switch
Flow-table
-----
Dpid          In Port  Src Mac  Dst Mac  Ether  Src IP  Dst IP
Proto  Src Port  Dst Port  App Name  Actions
-----  -
00:00:00:1a:1e:01:bf:70 *          *          *          0x806  *          *
*          *          *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:bf:70 *          *          *          0x86dd *          *
58        135        *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:bf:70 *          *          *          0x86dd *          *
58        136        *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:ae:28 *          *          *          0x86dd *          *
58        135        *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:ae:28 *          *          *          0x86dd *          *
58        136        *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:ae:28 *          *          *          0x806  *          *
*          *          *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:99:e0 *          *          *          0x806  *          *
*          *          *          routing_switch output=normal,output=controller
00:00:00:1a:1e:01:99:e0 *          *          *          0x86dd *          *
58        135        *          routing_switch output=normal,output=controller
```

```

00:00:00:1a:1e:01:99:e0 * * * 0x86dd * *
58 136 * routing_switch output=normal,output=controller
00:00:00:0b:86:9a:4e:77 * * * 0x86dd * *
58 135 * routing_switch output=normal,output=controller
00:00:00:0b:86:9a:4e:77 * * * 0x86dd * *
58 136 * routing_switch output=normal,output=controller
Flow-table
-----
Dpid In Port Src Mac Dst Mac Ether Src IP Dst IP
Proto Src Port Dst Port App Name Actions
-----
00:00:00:0b:86:9a:4e:77 * * * 0x806 * * *
* * routing_switch output=normal,output=controller
Total number of flows: 12

```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller

```
show openflow-controller flows
  app-name <name>
  dpid <dp-id>
  flow-cookie
  flow-id
```

Description

The command displays the flow information of the OpenFlow Controller on Mobility Conductor.

Parameter	Description
app-name <name>	Displays the name of app that installed the flow.
dpid <dp-id>	The dpid of the switch.
flow-cookie	Displays the dump flow by a specified cookie.
flow-id	Displays the dump flow by a specified flow-id.

Example

The following command displays the OpenFlow Controller flows details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller flows
Flow 1 :
cookie : 112589990684262402 (1900000000000002)
flow-id : 1913000000005643
flow-group-id : 1913000000000003
status : Install-Confirmed
dpid : 00:00:00:1a:1e:00:d9:40
priority : 65535
hard timeout : 0
idle timeout : 0
packet count : 0
byte count = 0
app name : routing_switch
Match :
eth-type : 0x86dd
ip-protocol : 58
icmpv6_type : 136
Actions : output=normal,output=controller
Flow 2 :
cookie : 112589990684262403 (1900000000000003)
flow-id : 18ef000000005641
flow-group-id : 18ef000000000001
status : Install-Confirmed
dpid : 00:00:00:1a:1e:00:d9:40
```



```
priority : 65535
hard timeout : 0
idle timeout : 0
packet count : 0
byte count = 0
app name : topology
Match :
eth-type : 0x800
src IP : 1.1.1.1
dst IP : 2.2.2.2
ip-protocol : 97
Actions : output=controller
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller forwarding-db

```
show openflow-controller forwarding-db  
mac-address <mac-address>
```

Description

The command displays data per client for the forwarding database.

Parameter	Description
mac-address	Displays the mac address of the host.

Example

The following command displays the OpenFlow Controller forwarding-db details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller forwarding-db  
FDB  
---  
MAC                Wireless  Dpid          Created/Updated  
                -----  ---          -----  
                ---  
58:94:6b:7a:a4:24  TRUE     00:00:00:1a:1e:00:d9:40  Mon Oct 19 08:43:58  
2020/Mon Oct 19 08:43:58 2020 *  
00:1a:1e:11:89:00  FALSE    00:00:00:1a:1e:00:d9:40  Thu Oct 15 23:27:49  
2020/Thu Oct 15 23:27:49 2020 10.17.24.17  
Total number of entries in fdb: 2
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller hosts

```
show openflow-controller hosts
  dpid <dp-id>
  ip-address <ip>
  mac-address <mac>
```

Description

The command displays OpenFlow host configuration information on Mobility Conductor. You can also filter the view by datapath ID, IP address or MAC address of the host.

Parameter	Description
dpid <dp-id>	Displays the dpid of the switch.
ip-address <ip>	Displays the ip address of the host.
mac-address <mac>	Displays the mac address of the host.

Example

The following command displays the OpenFlow Controller hosts details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller hosts
Hosts
-----
IP          MAC          Wireless  Dpid
  Port No  Port MAC
--          ---          -
-----
10.17.24.17 00:1a:1e:11:89:00 false
00:00:00:1a:1e:00:d9:40 2 00:1a:1e:00:d9:41
fe80::94f9:65f:b817:2f52 58:94:6b:7a:a4:24 True
00:00:00:1a:1e:00:d9:40 22 ac:a3:1e:c0:8b:22
Total number of hosts: 2
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller links

```
show openflow-controller links  
  dpid <dp-id>
```

Description

The command displays OpenFlow links on Mobility Conductor. You can also filter the output based on the datapath ID of the OpenFlow instance.

Parameter	Description
dpid <dp-id>	Displays the dpid of the switch.

Example

The following command displays the OpenFlow Controller links details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller links  
Links  
-----  
From Dpid                From Port  To Dpid                To Port  Status  
-----  
00:00:00:1a:1e:00:d9:40  2          00:00:00:1a:1e:00:d9:44  22
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller ports

```
show openflow-controller ports  
  dpid <dp-id>
```

Description

The command displays the OpenFlow ports configured on Mobility Conductor. You can also filter the output based datapath ID of the OpenFlow instance.

Parameter	Description
dpid <dp-id>	Displays the dpid of the switch.

Example

The following command displays the OpenFlow port configuration on Mobility Conductor:

```
(host) [mynode] #show openflow-controller ports  
Ports  
-----  
Dpid          TX Packets  RX Packets  Port No  Name          MAC          Status  
-----  
00:00:00:1a:1e:01:bf:70 13670286 14405254 1      GE0/0/0      00:1a:1e:01:bf:71  Up  
00:00:00:1a:1e:01:ae:28 7195701 8124898 2      GE0/0/0      00:1a:1e:01:ae:29  Up  
00:00:00:1a:1e:01:99:e0 9064283 9704562 3      PC0          00:1a:1e:01:99:e0  Up  
00:00:00:0b:86:9a:4e:77 0 0 11     GE0/0/8      00:0b:86:9a:4e:80  Down  
00:00:00:0b:86:9a:4e:77 0 0 12     GE0/0/9      00:0b:86:9a:4e:81  Down  
00:00:00:0b:86:9a:4e:77 0 0 13     GE0/0/10     00:0b:86:9a:4e:82  Down  
00:00:00:0b:86:9a:4e:77 0 0 14     GE0/0/11     00:0b:86:9a:4e:83  Down  
00:00:00:0b:86:9a:4e:77 0 0 15     GE0/0/12     00:0b:86:9a:4e:84  Down  
00:00:00:0b:86:9a:4e:77 0 0 16     GE0/0/13     00:0b:86:9a:4e:85  Down  
00:00:00:0b:86:9a:4e:77 0 0 17     GE0/0/14     00:0b:86:9a:4e:86  Down  
00:00:00:0b:86:9a:4e:77 0 0 18     GE0/0/15     00:0b:86:9a:4e:87  Down  
00:00:00:0b:86:9a:4e:77 0 0 19     GE0/0/16     00:0b:86:9a:4e:88  Down
```



```

00:00:00:0b:86:9a:4e:77 20      GE0/0/17      00:0b:86:9a:4e:89 Down
0 0
00:00:00:0b:86:9a:4e:77 21      PC0           00:0b:86:9a:4e:77 Down
0 0
00:00:00:0b:86:9a:4e:77 7       GE0/0/4       00:0b:86:9a:4e:7c Down
0 0
00:00:00:0b:86:9a:4e:77 6       GE0/0/3       00:0b:86:9a:4e:7b Down
0 0
00:00:00:0b:86:9a:4e:77 5       GE0/0/2       00:0b:86:9a:4e:7a Down
0 0
00:00:00:0b:86:9a:4e:77 9       GE0/0/6       00:0b:86:9a:4e:7e Down
0 0
00:00:00:0b:86:9a:4e:77 10      GE0/0/7       00:0b:86:9a:4e:7f Down
0 0
00:00:00:0b:86:9a:4e:77 8       GE0/0/5       00:0b:86:9a:4e:7d Down
0 0
00:00:00:0b:86:9a:4e:77 4       GE0/0/1       00:0b:86:9a:4e:79 Down
0 0
00:00:00:0b:86:9a:4e:77 2       GE0/0/0       00:0b:86:9a:4e:78 Up
4637389      4551706

```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller resource

show openflow-controller resource

Description

The command displays the OpenFlow resource usage information on Mobility Conductor.

Example

The following command displays the OpenFlow resource usage information on Mobility Conductor:

```
(host) [mynode] #show openflow-controller resource
Resource Usage
-----
Process                               PID  Uptime                               RSS (kB)  PSS (kB)
USS (kB)  Data (kB)
-----  -----
-----  -----
switch_daemon.0xb869a4e77             8028  1 (d) 10 (h) 45 (m) 13 (s)  7316     3997
3896      4076
switch_daemon.0x1a1e0199e0            8010  1 (d) 10 (h) 45 (m) 15 (s)  5700     2388
2288      2360
switch_daemon.0x1a1e01ae28            7944  1 (d) 10 (h) 45 (m) 25 (s)  5736     2460
2360      2492
switch_daemon.0x1a1e01bf70            7912  1 (d) 10 (h) 45 (m) 31 (s)  6604     3285
3184      3284
switch_manager                         6429  1 (d) 10 (h) 47 (m) 57 (s)  5388     2658
2600      2568
event_dispatcher                       6423  1 (d) 10 (h) 47 (m) 57 (s)  6196     2308
2116      18808
packetin_dispatcher                   6419  1 (d) 10 (h) 47 (m) 57 (s)  7092     3421
3232      110112
flow_manager                           6412  1 (d) 10 (h) 47 (m) 57 (s) 14880     10993
10796     115104
topology                               6391  1 (d) 10 (h) 47 (m) 58 (s)  5992     2267
2080      18676
routing_switch                         6408  1 (d) 10 (h) 47 (m) 58 (s)  8848     4850
4644      86704
topology_discovery                    6400  1 (d) 10 (h) 47 (m) 58 (s)  6616     2912
2720      19376
Total Processes: 11  RSS: 80368 (kB)  PSS: 41539 (kB)  USS: 39916 (kB)
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller statistics

```
show openflow-controller statistics
  process-name <name>
```

Description

The command displays the OpenFlow statistics information. You can also filter the output based on any of the following process names - flow_manager, topology, topology_discovery, routing_switch, switch_manager, packetin_dispatcher, and event_dispatcher.

Parameter	Description
process-name	Displays the OpenFlow statistics information for the process selected.

Example

The following command displays the OpenFlow Controller statistics details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller statistics
Debug-stats
-----
Process-name      Counter-name      Value  Current-Rate (last
10 seconds) Max-Rate
-----
-----
topology          send_success      403    0
                    5
topology_discovery send_success      2      0
                    2
topology_discovery send_dequeue      1      0
                    1
topology_discovery send_enqueue      1      0
                    1
routing_switch    send_success      9988   0
                    3
routing_switch    send_dequeue      1      0
                    1
routing_switch    send_enqueue      1      0
                    1
flow_manager      send_dequeue      1      0
                    1
flow_manager      send_enqueue      1      0
                    1
packetin_dispatcher send_dequeue      1      0
                    1
```

packetin_dispatcher	send_enqueue	1	0
1			
switch_manager	send_success	14890	0
4			
flow_manager	send_success	20226	0
35			
topology	app_service_event_type_config	3	0
0			
topology_discovery	app_service_event_type_config	3	0
0			
routing_switch	app_service_event_type_config	3	0
0			
flow_manager	app_service_event_type_config	3	0
0			
packetin_dispatcher	app_service_event_type_config	3	0
0			
event_dispatcher	app_service_event_type_config	3	0
0			
switch_manager	cleanup_listener_info_socket	2	0
0			

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller summary

```
show openflow-controller summary
by- dpid <dp-id>
```

Description

The command displays the OpenFlow summary information on Mobility Conductor. You can also filter the output based datapath ID of the OpenFlow instance.

Parameter	Description
by dpid <dp-id>	Displays the summary information of the dpid selected.

Example

The following command displays the OpenFlow Controller summary details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller summary
Total number of switches (UP): 1
Total number of switches (DOWN): 0
Total number of ports: 25
Total number of links: 0
Total number of hosts: 2
Total number of ip hosts: 2
Total number of flows: 26
Openflow connection on MD: Enabled
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-controller switches

```
show openflow-controller switches
  details
```

Description

The command displays the OpenFlow Controller configuration information on . In addition, you can view information such as flows, flow tables, hosts, and statistics related to OpenFlow Controller on Mobility Conductor.

Parameter	Description
details	Displays the details of the OpenFlow switches on the Mobility Conductor.

Example

The following command displays the OpenFlow Controller switches details on Mobility Conductor:

```
(host) [mynode] #show openflow-controller switches
Switches
-----
Dpid          IP          Version  Status  Auxiliary-
Status/Id    Capabilities  --      -----  -----
-----
00:00:00:1a:1e:01:bf:70  192.168.200.16:43364  v1.3    Up      Down/0
      Flow stats, Table stats, Port stats, Queue Stats  Aruba Networks,
      Inc. Aruba7240 8.0.0.0-svcs-ctrl UCC-Sol-7240 BC0003370
00:00:00:1a:1e:01:ae:28  192.168.200.14:45570  v1.3    Up      Down/0
      Flow stats, Table stats, Port stats, Queue Stats  Aruba Networks,
      Inc. Aruba7210 8.0.0.0-svcs-ctrl UCC-Sol-7210 BA0009702
00:00:00:1a:1e:01:99:e0  192.168.200.15:52066  v1.3    Up      Down/0
      Flow stats, Table stats, Port stats, Queue Stats  Aruba Networks,
      Inc. Aruba7220 8.0.0.0-svcs-ctrl UCC-Sol-7220 BB0003406
00:00:00:0b:86:9a:4e:77  10.16.125.12:46797   v1.3    Up      Down/0
      Flow stats, Table stats, Port stats, Queue Stats  Aruba Networks,
      Inc. Aruba7010 8.0.0.0-svcs-ctrl UCC-BOC1  CG0001826
Total number of switches: 4
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show openflow-profile

```
show openflow-profile
```

Description

The command displays the OpenFlow profile information configured on the managed device.

Example

The following command displays the OpenFlow profile information on the managed device. Execute the following commands to verify OpenFlow profile configuration on managed devices:

```
(host) [md] #show openflow-profile
Openflow-profile "default"
-----
Parameter                               Value
-----
State                                    Enabled
Openflow mode                            passive
Openflow version                          v1.3
controller-ip                             10.16.125.115:6633
VLAN ID or range(s) of VLAN IDs          1,124,400,600
openflow tls                              Disabled
certificate-file                           none
key-file                                    none
ca-certificate-file                         none
```

Related Commands

Command	Description
openflow-profile	This command configures OpenFlow profile on the managed device

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on managed device.

show packages

show packages [supported|upgrade-history]

Description

This command displays information about the downloaded and active Loadable Service Module (LSM) service packages.

Parameter	Description
supported	Displays all packages supported by Mobility Conductor.
upgrade-history	Displays package installation logs.

Example

The following command lists all packages downloaded on a given Mobility Conductor:

```
(host) [mynode] #show packages

Packages
-----
Package      Name                               Version                               Build
Num  Built On  Package Version  Active
-----  -
-----  -
airgroup     default_airgroup_pkg               ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
airmatch     default_airmatch_pkg               ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
appRF        default_appRF_pkg                  ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
arm_cm       default_arm_cm_pkg                 ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
nbapi_helper default_nbapi_helper_pkg           ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
ucm          default_ucm_pkg                    ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
web_cc       default_web_cc_pkg                 ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES
wms          default_wms_pkg                    ArubaOS_MM_8.0.0.0-svcs-ctrl  55038
  Mon May 16 14:44:20 PST 2016  1                               YES

The following command lists all packages supported by a given Mobility
Conductor:
(host) [mynode] #show packages supported

Packages Supported
-----
Package Name  Version
```

```

-----
airgroup      1
ucm           1
wms           1
arm_cm        1
web_cc        1
nbapi_helper  1
airmatch      1
appRF         1

```

The following command displays the package installation logs:

```

(host) [mynode] #show packages upgrade-history

May 17 21:00:11 Copying files to airgroup dir
May 17 21:00:11 Creating symbolic link to mdns binary
May 17 21:00:11 Package default_airgroup_pkg installation was successfully
May 17 21:00:12 Copying files to ucm dir
May 17 21:00:12 Creating symbolic link to ucm binary
May 17 21:00:12 Package default_ucm_pkg installation was successfully
May 17 21:00:12 Copying files to wms dir
May 17 21:00:12 Creating symbolic link to wms binary
May 17 21:00:12 Package default_wms_pkg installation was successfully
May 17 21:00:12 Copying files to arm_cm dir
May 17 21:00:12 Creating symbolic link to arm binary
May 17 21:00:12 Package default_arm_cm_pkg installation was successfully
May 17 21:00:12 Copying files to web_cc dir
May 17 21:00:12 Creating symbolic link to web_cc binary
May 17 21:00:12 Package default_web_cc_pkg installation was successfully
May 17 21:00:12 Copying files to nbapi_helper dir
May 17 21:00:12 Creating symbolic link to nbapi_helper binary
May 17 21:00:12 Package default_nbapi_helper_pkg installation was
successfully
May 17 21:00:13 Copying files to airmatch dir
May 17 21:00:13 Copying airmatch binary
May 17 21:00:13 Package default_airmatch_pkg installation was successfully
May 17 21:00:13 Copying files to appRF dir
May 17 21:00:13 Creating symbolic link to appRF binary

```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show packet-capture

```
show packet-capture
  controlpath-pcap [hex]
  datapath-pcap [hex]
```

Description

Displays packet capture status on the controller.

Parameter	Description
controlpath-pcap [hex]	Displays controlpath packets captured in the local-file system.
datapath-pcap [hex]	Displays datapath packets captured in the local-file system.

Example

The output of this command shows the packet capture configuration details.

```
(host)[mynode] #show packet-capture
Active Capture Destination
-----
Destination      IP          1.2.3.4
Active Capture (Controlpath)
-----
Interprocess     Disabled
Sysmsg           Disabled
TCP              Enabled     Ports: 2
UDP              Enabled     Ports: 5
Other            Enabled
Active Capture (Datapath)
-----
Wifi-Client      Enabled     Mac: 00:0b:86:6d:47:6c   Filter: Decrypted
Ipsec            Enabled     Peer: 10.1.1.1
(host) (config) #show packet-capture-defaults
Default Capture Destination
-----
Destination      Local-Filesystem
Default Capture (Controlpath)
-----
Interprocess     Disabled
Sysmsg           Disabled
TCP              Enabled     Ports: 80 8080
UDP              Enabled     Ports: All
Other            Disabled
Default Capture (Datapath)
-----
Wifi-Client      Enabled     Mac: 00:0b:86:6d:47:6c   Filter: Encrypted
Ipsec            Disabled
```

Related Commands

Command	Description
packet-capture	This command enables or disables packet capturing and sets packet capturing options for a single packet capture session.
packet-capture-defaults	This command enables or disables packet capturing and defines a set of default packet capturing options on the control path for debugging purposes.
ap packet-capture	These commands manage WiFi packet capture (PCAP) on Aruba APs. The WiFi packets are encapsulated in a UDP header and sent to a client running a packet analyzer like Wildpacket's Airopeek, Omnipeek, or Wireshark.
no packet-capture	This command disables packet capturing for debugging.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show packet-capture-defaults

show packet-capture-defaults

Description

Displays the status of default packet capture options.

Example

The output of this command shows packet capture status.

```
(host) # show packet-capture-defaults

Current Active Packet Capture Actions(current switch)
=====
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.

Packet Capture Defaults(across switches and reboots if saved)
=====
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.
```

Related Commands

Command	Description
packet-capture	This command enables or disables packet capturing and sets packet capturing options for a single packet capture session.
packet-capture-defaults	This command enables or disables packet capturing and defines a set of default packet capturing options on the control path for debugging purposes.
ap packet-capture	These commands manage WiFi packet capture (PCAP) on Aruba APs. The WiFi packets are encapsulated in a UDP header and sent to a client running a packet analyzer like Wildpacket's Airopeek, Omnippeek, or Wireshark.
no packet-capture	This command disables packet capturing for debugging.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show pan

```
show pan
  active-profile
  debug
  profile
  state
  statistics
```

Description

This command shows the active PAN profiles. Click parameter links to view the corresponding show commands.

Parameter	Description
active-profile	Show the Palo Alto Networks Active Profile.
debug	Show PAN debug information.
profile	Show a Palo Alto Networks Servers Profile
state	Show PAN Interface connection state.
statistics	Show PAN Interface Statistics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan active-profile

```
show pan active-profile
```

Description

This command shows the active PAN firewall profile at the managed device level.

Example

Issue this command to show the current active PAN firewall profile running on the managed device.

```
(host)[node]#show pan active-profile
Palo Alto Networks Active Profile
-----
Parameter                               Value
-----
Active Palo Alto Networks profile      PAN-Group-1
```

Related Commands

Command	Description
pan active-profile	This command makes a Palo Alto Network profile active from a set of profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan debug

show pan debug

Description

This command shows PAN debug information.

Example

The following command shows the output of show pan debug command.

```
(host)[node]#show pan debug
Palo Alto Networks Interface Debug Information
-----
User Changed   User Deleted   User Deactivated   Refresh   Login Reqts   Logout
Reqts   Refresh Reqts   No UserName   No Change   No Deletion
-----
0         0         5         0         0         0         931     0         0
0         0         0         0         0         5
Per-PAN server Debug Information
-----
PAN Server   State   User-ID Reqts   Sent   Skipped   Success   Failure   Last
Error
-----
-
Work Factory Debug Information
-----
Mgmt Queue   Reqt Queue
-----
0             0(8192)
PAN Local UID-Table - total:0(0) cur:3 ref:4
=====
0         0         0         0         0         0         0         0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan profile

```
show pan profile
```

Description

This command displays configured settings for integrating a branch controller with a Palo Alto Networks (PAN) firewall.

Example

Issue this command to see the connection status of the PAN firewalls associated with the controller.

```
(host)[node]#show pan profile PAN-Group-1

Palo Alto Networks Servers Profile "PAN-Group-1"
-----
Parameter                               Value
-----
Palo Alto Networks Firewall             1.2.3.4:443 abc/*****
Palo Alto Networks Firewall             2.2.2.2:123 2222/*****
Palo Alto Networks Firewall             3.3.3.3:333 3333/*****
Palo Alto Networks Firewall             1.1.1.1:443 admin/*****
```

Related Commands

Command	Description
pan active-profile	This command selects an active Palo Alto Network (PAN) profile from a set of profiles.
pan profile	This command configures a Palo Alto Networks (PAN) profile to allow a managed device to communicate with a PAN firewall.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan state

```
show pan state
```

Description

This command shows the current connection status of PAN firewalls associated with the controller.

Example

The following command shows the output of show pan state command.

```
(host)[node] #show pan state
Palo Alto Networks Servers Connection State[PAN-Group-1]
-----
Firewalls      State                               Last Error
-----      -
1.2.3.4:443    DOWN
2.2.2.2:123    UP[11/25/13 12:45:49]Established
3.3.3.3:333    UP[11/25/13 12:45:48]Established
1.1.1.1:443    UP[11/25/13 12:45:50]Established
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan statistics

show pan statistics

Description

This command shows PAN firewall interface statistics. Use this command to see the following interface statistics.

Example

The output of this command shows the show pan statistics configuration details.

```
(host)[node](config) #show pan statistics
Palo Alto Networks Interface Statistics Summary
-----
Login Reqts   Logout Reqts   Refresh Reqts
-----
0             0             0
Per-PAN server Statistics Summary
-----
PAN Server      User-ID Reqts   Sent   Skipped   Success   Failure   Last Error
-----
1.2.3.4:443    0             0     0         0         0         
```

Parameter	Description
Palo Alto Networks Interface Statistics Summary	
Login Reqts	Total number of login requests.
Logout Reqts	Total number of logout requests.
Refresh Reqts	Total number of refresh requests.
Per-PAN server Statistics Summary	
PAN Server	The PAN Server IP address.
User-ID Reqts	Total number of login, logout, and refresh requests.
Sent	Number of requests sent.
Skipped	Number of requests skipped.
Success	Number of requests successfully handled.
Failure	Number of requests that were not successfully received.

Parameter	Description
Last Error	The last failure error received.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show pan-options

show pan-options

Description

This command displays configured options to integrate a managed device with a Palo Alto Networks (PAN) firewall.

Issue this command to view Palo Alto Networks firewall integration settings for a managed device. Note that the PAN firewall integration feature can only be used on a managed device when used in conjunction with the managed device uplink VLAN manager feature, which must be enabled using the [uplink](#) command in the Mobility Conductor CLI.

Examples

The output of this command shows the show pan-options configuration details.

```
(host)[node]# show pan-options
Configure Palo Alto Networks options
-----
Parameter                                     Value
-----
Portal IP for Palo Alto Networks Global Protect portal 172.16.100.1 cert
cert_LSVPN_CA_7 username aruba123 password *****
```

The output of this command contains the following parameters:

Parameter	Description
Parameter	This column displays the Palo Alto Network (PAN) parameter.
Value	This column contains displays the following parameters for Palo Alto firewall integration feature: <ul style="list-style-type: none">portal-ip <ip-addr>: The IP address of the firewall management portalcert <cert-name>: Name of the self-signed or external certification authority (CA) certificate to sign the managed device and gateway server certificates

Related Commands

Command	Description
pan active-profile	This command selects an active Palo Alto Network (PAN) profile from a set of profiles.
pan profile	This command configures a Palo Alto Networks (PAN) profile to allow a managed device to communicate with a PAN firewall.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show papi-security

show papi-security

Description

This command shows a configured papi-security profile.

The `papi-security` command is used to enforce advanced security options and provides an enhanced level of security.

The **Parameter** column displays the PAPI Key and Enhanced security mode parameters. The **Value** column displays a Papi key value (encrypted) and indicates whether the Enhanced security mode is enabled or disabled.

```
(host)[mynode] #show papi-security

PAPI Security Profile
-----
Parameter                Value
-----
PAPI Key                  *****
Enhanced security mode    Enabled
```

Parameter	Description
PAPI Key	The key string. The key authenticates the messages between systems. 10-64 characters
Enhanced security mode	Indicates if the enhanced security mode is enabled or disabled. This mode causes the system to reject messages when an incorrect key is used. Disabled

Related Commands

Command	Description
papi-security	This command enforces advanced security options and provides an enhanced level of security.

Command History

Release	Modification
ArubaOS 8.0.1 .0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show papi kernel-socket-stats

show papi kernel-socket-stats

Description

This command shows the state of UDP PAPI sockets in the kernel.

The following example shows partial output of this command.

```
(host)[node] #show papi kernel-socket-stats Kernel PAPI Statistics
Port
RxSockbufHimark CurRxQLen MaxRxQLen Drops RxSockbufSize
9344 (9344)
    7104      0      3      0      2097152
8449 (Utility Process)
    0      0      0      0      2097152
9345 (9345)
    0      0      0      0      2097152
514 (514)
    0      0      0      0      2097152
9476 (9476)
    0      0      0      0      2097152
9348 (9348)
    0      0      0      0      2097152
9220 (9220)
    0      0      0      0      2097152
8453 (Control Plane Security Daemon)
    2368      0      1      0      2097152
9222 (9222)
    0      0      0      0      2097152
9478 (9478)
    0      0      0      0      2097152
8455 (Spectrum Process)
    0      0      0      0      2097152
8456 (STM Monitoring)
    0      0      0      0      2097152
9224 (9224)
    0      0      0      0      2097152
9481 (9481)
    0      0      0      0      2097152
9482 (9482)
    0      0      0      0      2097152
8458 (Arci cli helper server)
    0      0      0      0      2097152
9226 (9226)
    0      0      0      0      2097152
9483 (9483)
    0      0      0      0      2097152
9355 (9355)
    0      0      0      0      2097152
8459 (WMS Monitoring)
    0      0      0      0      2097152
```


9484 (9484)					2097152
0	0	0	0		
9485 (9485)					2097152
0	0	0	0		
9486 (9486)					2097152
0	0	0	0		
9359 (9359)					2097152
0	0	0	0		
9231 (9231)					2097152
0	0	0	0		

Related Commands

Command	Description
papi-security	The papi-security command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or config mode on Mobility Conductor.

show perf-test reports

```
show perf-test reports
  ap {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
  controller
```

Description

Use this command under the guidance of Aruba technical support to view the results of an Iperf throughput test launched from an AP or controller.

Tests launched in server mode do not generate reports. Only 130 Series, 220 Series, and AP-105 access points connected to a7200 Series controller support this feature.

Parameter	Description
ap	Display the results of an Iperf throughput test launched from an AP.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IPv4 address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
controller	Display the results of an Iperf throughput test launched from a controller.

Related Commands

Command	Description
perf-test server	Use this command under the guidance of Aruba technical support to launch an Iperf throughput test.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
7200 Series controllers	Base operating system.	Enable mode on Mobility Conductor.

show phonehome

```
show phonehome
  global
  history
  report-status
  stats
```

Description

Use this command to view current configuration settings and debugging statistics for the PhoneHome automatic reporting feature.

The automatic reporting feature, also known as *PhoneHome*, allows a controller to securely contact Aruba support servers over the Internet to report events such as hardware failures, software malfunctions, and other critical events. When the PhoneHome automatic reporting feature is enabled, the controller sends Aruba support weekly reports about the controller's configuration, licenses, software and hardware versions, and any software malfunctions via a secure email.

Parameter	Description
global	Show whether the PhoneHome service and auto-reporting is enabled or disabled, and display current HTTPS or SMTP settings for this feature.
history	Issue this command under the guidance of Aruba support troubleshoot PhoneHome automatic reporting.
report-status	Issue this command under the guidance of Aruba support troubleshoot PhoneHome automatic reporting.
stats	Include this parameter to show the number of weekly schedule or manual reports successfully sent to Activate or the SMTP server, the number of times the controller attempted to retry sending a report, and the number of reports that failed after one or more retry attempts, and

Example

The following command displays global phonehome settings:

```
(host)[mynode] #show phonehome global
PhoneHome information:
PhoneHome Service:      Disabled
PhoneHome Auto-Report:  Disabled
Local SMTP server:     192.0.2.10:25
SMTP From Email:       admin@example.com
```

Max Attachment Size: 10 MB
SMTP Authen User: John_Smith

Related Commands

Command	Description
phonehome	This command configures the PhoneHome auto reporting feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Conductor.

show poe

```
show poe [<slot/module/port>]
```

Description

Displays the PoE status of all or a specific port on the controller.

Example

The output of this command shows the PoE status of the specified slot, module and port.

```
(host) [mynode] # show poe 0/0/2

PoE Status
-----
Port      Status  Voltage (mV)  Current (mA)  Power (mW)
-----
GE 0/0/2  Off      N/A           N/A           N/A
```

Related Commands

Command	Description
ap enet-link-profile	This command configures an AP Ethernet link profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port

```
show port
  link-event
  monitor
  nic-registers
  stats
  status
  trusted
  tunneled-node
  untrusted-vlan
  xsec
```

Description

This command shows the port settings. Click parameter links to view the corresponding show commands.

Parameter	Description
link-event	Show port link up/down event counters.
monitor	Show monitor port configuration.
<code>nic-registers</code>	Show port nic registers values.
stats	Show physical port statistics.
status	Show physical port status.
trusted	Show the trusted ports.
tunneled-node	Show the tunneled node ports.
untrusted-vlan	Show untrusted port vlan.
xsec	Show xsec ports.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show policy-domain group-profile

show policy-domain group-profile

Description

This command shows the details of the policy domain profile.

Example

The output of the `show policy-domain group-profile` displays the policy domain profile

```
(host) #show policy-domain group-profile
Policy Domain Profile List
-----
Name  Profile Status
----  -
test
Total:1
```

Related Commands

Command	Description
policy-domain	This command configures a policy domain profile to apply role-based ACL for users present in different controllers.

Command History

Version	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config modes on Managed Devices.

show port link-event

```
show port link-event
```

Description

Displays the link status on each of the port, on the controller.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode] # show port link-event

Slot/Port  UP      DOWN
-----  --      ----
 0/0/0      1       0
 0/0/2     49751   49750
 0/0/3     2589    2588
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port monitor

show port monitor

Description

Displays the list of ports that are configured to be monitored.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode]# show port monitor

Monitor Port   Port being Monitored
-----
FE 1/10        FE 1/20
```

Related Commands

Command	Description
interface gigabitethernet	This command configures a GigabitEthernet interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port stats

show port stats [<slot/module/port>]

Description

Displays the activity statistics on each of the port on the controller.

Parameter	Description
<slot/module/port>	Physical port in <slot>/<module>/<port> format.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode] # show port stats

Port Statistics
-----
Port          PacketsIn  PacketsOut  BytesIn   BytesOut  InputErrorBytes
OutputErrorBytes  CRCErrors  RxNoMbuf
-----
GE 0/0/0      745969    18810      86791364  10599122  0
              0          0
GE 0/0/1      0          0          0         0         0
              0          0
GE 0/0/2      0          0          0         0         0
              0          0
```

The output of this command includes the following parameters:

Parameter	Description
Port	Displays the physical port on the controller.
PacketIn	Indicates the total number of incoming packets to the port.
PacketOut	Indicates the total number of outgoing packets from the port.
BytesIn	Indicates the total number of incoming data (in bytes) to the port.
BytesOut	Indicates the total number of outgoing data (in bytes) from the port.
InputErrorBytes	Indicates input error bytes on the port.

Parameter	Description
OutputErrorBytes	Indicates the output error bytes on the port.
CRCErrors	Indicates the Cyclic Redundancy Check (CRC) errors on the port.
RxNoMbuf	Indicates the receive buffer allocated to handle traffic bursts.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

show port status

show port status [<slot/module/port>]

Description

Displays the status of all ports on the controller.

Parameter	Description
<slot/module/port>]	Physical port in <slot>/<module>/<port> format.

Example

The output of this command shows the status of all ports in the controller.

```
(host)[mynode]# show port status
Port Status
-----
Slot-Port  PortType  AdminState  OperState  PoE  Trusted  SpanningTree
PortMode  Speed    Duplex    PortError
-----
- - - - -
0/0/0      GE        Enabled     Up          N/A  Yes      Disabled     Trunk
 10 Gbps   Full     -
0/0/1      GE        Disabled    Down        N/A  Yes      Disabled     Access
 Auto     Auto     -
```

The output of this command includes the following parameters:

Parameter	Description
Slot-Port	Physical port in <slot>/<module>/<port> format.
PortType	Displays the type of physical port. <ul style="list-style-type: none">▪ FE: Fast Ethernet▪ GE: Gigabit Ethernet▪ PC: Port Channel
AdminState	Indicates if the physical port is enabled or disabled.
OperState	Indicates if the current status of the physical port is up or down.
PoE	Indicates if the physical port is Power over Ethernet (PoE) enabled.

Parameter	Description
Trusted	Indicates if the physical port is trusted.
SpanningTree	Indicates the state of spanning tree.
PortMode	Indicates the port mode of the physical port.
Speed	Indicates the port speed.
Duplex	Indicates the direction of traffic.
PortError	Indicates is there is an error in the physical port.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port trusted

show port trusted

Description

Displays the list of ports configured with trusted profiles.

Example

The output of this command shows the list of ports with trusted profile.

```
(host)[mynode]# show port trusted
FE 1/0
FE 1/1
FE 1/2
FE 1/3
GE 1/24
GE 1/25
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port tunneled-node

show port tunneled-node

Description

This command shows the tunneled node ports.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command shows the tunneled node ports.

```
(host) [mynode] #show port tunneled-node
GE 0/0/4
GE 0/0/7
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show port xsec

```
show port xsec
```

Description

Displays the list of xSec enabled ports.

Example

The output of this command shows the list of xSec enabled ports.

```
(host)[mynode] #show port xsec

Xsec Ports
-----
Interface  xsec vlan  state
-----  -
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show port untrusted-vlan

show port untrusted-vlan

Description

This command shows untrusted port VLANs.

Example

The following command shows untrusted port VLANs,

```
(host)[mynode] #show port untrusted-vlan
Port Untrusted Vlan Table
-----
Name: Pc 0
Vlan(s): 1-4094
Name: Pc 1
Vlan(s): 1-4094
Name: Pc 2
Vlan(s): 1-4094
```

Related Commands

Command	Description
show datapath	This command displays system statistics for a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Managed Device.

show priority-map

show priority-map

Description

Displays the list of priority maps on a interface.

Example

The output of this command shows the priority maps configured on all interfaces.

```
(host)[node] # show priority-map

Priority Map
-----
ID   Name      DSCP-TOS  DOT1P-COS
--   -
1    my-map    4-20,60   4-7
```

Related Commands

Command	Description
priority-map	This command configures the ToS and CoS values used to map traffic into high priority queues.
interface gigabitethernet	This command configures a GigabitEthernet interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show processes

show processes [sort-by {cpu | memory}]

Description

Displays the list of all system process running on the managed device. You can sort the list either by CPU intensive or memory intensive processes.

Parameter	Description
sort-by	Add a sort filter to the output
cpu	This will sort output based on CPU usage.
memory	This will sort output based on memory usage.

Example

The output of this command shows list of system processes sorted by CPU usage.

```
(host) [mynode] (config) # show processes

%CPU S   PID  PPID  VSZ  RSS  F  NI  START      TIME      EIP  CMD
3.7 S   595   517 20908 12184 040 0 Apr24 03:39:04 303a4fa8
/mswitch/bin/fpapps
0.2 S 12354  410  1028  296 000 0 02:13 00:00:00 30087fa8 sleep 10
0.1 S   536  441 12012 7264 040 0 Apr24 00:09:08 100e4a74
/mswitch/mysql/libexec/mysqld --basedir=/mswitch/mysql --datadir=/var/
0.0 S    2    1    0    0 040 0 Apr24 00:00:00 00000000 [keventd]
0.0 S    4    0    0    0 040 0 Apr24 00:00:00 00000000 [kswapd]
0.0 S    6    0    0    0 040 0 Apr24 00:00:00 00000000 [kupdated]
0.0 S   57    1    0    0 040 0 Apr24 00:00:00 00000000 [kjournald]
0.0 S   67    1  1036  424 000 0 Apr24 00:00:00 30087fa8 /bin/sh
/mswitch/bin/syslogd_start
0.0 S    1    0  1028  384 100 0 Apr24 00:00:12 30087fa8 init
0.0 S   397    1  1732  804 100 0 Apr24 00:00:00 30152fa8
/mswitch/bin/nanny /mswitch/bin/nanny_list 0
0.0 S   399  397 14140 10172 100 0 Apr24 00:00:16 303c8fa8
/mswitch/bin/arci-cli-helper
0.0 S   402    1   768  268 040 0 Apr24 00:00:00 30060fa8 /sbin/tftpd -s
-l -u nobody /mswitch/sap
0.0 S    69   67  1404  752 100 0 Apr24 00:01:27 300d3fa8
/mswitch/bin/syslogd -x -r -n -m 0 -f /mswitch/conf/syslog.conf
0.0 S   407  397  3100 1028 100 0 Apr24 00:00:00 302a0fa8
/mswitch/bin/packet_filter
0.0 S   408  397   4296 1340 100 0 Apr24 00:00:00 30339fa8
/mswitch/bin/certmgr
0.0 R    3    0    0    0 040 19 Apr24 00:00:01 00000000 [ksoftirqd_
CPU0]
```

```

0.0 S  453   397   700  284 000   0 Apr24 00:01:20 30087fa8
/mswitch/bin/msgHandler -g
0.0 S  468   397  1236  492 100   0 Apr24 00:00:00 300f8fa8
/mswitch/bin/pubsub
0.0 S  484   397 18456 14064 100   0 Apr24 00:00:19 303c8fa8
/mswitch/bin/cfgm

```

Related Commands

Command	Description
process restart	This command restarts a process and optionally creates a core file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show process fpapps

```

show process fpapps
  message-queue-stats
  task-stats
  timer-stats

```

Description

Displays the information from Level7's layer2/layer3 module.

Parameter	Description
message-queue-stats	Displays fpapps internal message queue operations statistics.

Parameter	Description
task-stats	Displays fpapps internal OS API tasks statistics.
timer-stats	Displays fpapps internal timer module statistics.

Example

This example shows output of the `show process fpapps task-stats` command.

```
(host) [mynode] (config) #show process fpapps task-stats

Level7 Fastpath OS-API task statistics
-----
Name                High Contentions  Contention peak(msec)  Contention peak
event  Contention peak time
-----  -----
-----  -----
sosFpThread         0                    2                    Lock
      Wed Nov  2 09:43:15 2022
tAticThread0        0                    0                    <Not set>
      <Not-set>
tAticTimer0         0                    0                    <Not set>
      <Not-set>
IpFwdTask           0                    11                   Unlock
      Tue Nov  1 17:21:51 2022
IpProcTask          0                    0                    <Not set>
      <Not-set>
dotldTimer          0                    1                    Unlock
      Tue Nov  1 17:22:42 2022
dotldRecv           0                    0                    <Not set>
      <Not-set>
fdbTask             0                    0                    <Not set>
      <Not-set>
PhyTask             0                    0                    <Not set>
      <Not-set>
osapiTimer          0                    0                    <Not set>
      <Not-set>
nim_t               0                    1                    Lock
      Tue Nov  1 17:21:50 2022
dtlTask             0                    1                    Unlock
      Tue Nov  1 17:29:46 2022
miscFpappsPoeStats 0                    0                    <Not set>
      <Not-set>
miscFpapps          0                    7                    Lock
      Tue Nov  1 17:21:51 2022
netlinkInterface    0                    0                    <Not set>
      <Not-set>
t0x40bb15          0                    6                    Unlock
      Tue Nov  1 17:21:50 2022
```

Related Commands

Command	Description
process restart	This command restarts a process and optionally creates a core file.
process monitor	The process monitor validates the integrity of processes every 120 seconds. If a process does not respond during three consecutive 120-second timeout intervals, that process is flagged as nonresponsive and the process monitor will create a log message, restart the process or reboot the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show process monitor statistics

show process monitor statistics

Description

Displays the current status of all the processes running under the process monitor watchdog.

Example

A partial example of the output of this command is shown below:

```
(host) [mynode] (config) #show process monitor statistics

Process Monitor Statistics
-----
Name                               State           Restarts  Timeout Value
-----
-----
/mswitch/bin/arci-cli-helper       PROCESS_RUNNING 0          120         3
/mswitch/bin/fpcli                 PROCESS_RUNNING 0          120         3
/mswitch/bin/packet_filter         PROCESS_RUNNING 0          120         3
/mswitch/bin/certmgr               PROCESS_RUNNING 0          120         3
/mswitch/bin/dbstart               PROCESS_RUNNING 0          120         3
/mswitch/bin/cryptoPOST            PROCESS_RUNNING 0          120         3
/mswitch/bin/sbConsoled            PROCESS_RUNNING 0          120         3
/mswitch/bin/pubsub                PROCESS_RUNNING 0          120         3
/mswitch/bin/cfgm                  PROCESS_RUNNING 0          120         3
/mswitch/bin/syslogdwrap           PROCESS_RUNNING 0          120         3
/mswitch/bin/aaa                   PROCESS_RUNNING 0          120         3
/mswitch/bin/fpapps                PROCESS_RUNNING 0          120         3
/mswitch/bin/pim                   PROCESS_RUNNING 0          120         3
/mswitch/bin/lic
```

Related Commands

Command	Description
process restart	This command restarts a process and optionally creates a core file.
process monitor	The process monitor validates the integrity of processes every 120 seconds. If a process does not respond during three consecutive 120-second timeout intervals, that process is flagged as nonresponsive and the process monitor will create a log message, restart the process or reboot the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile

```
show profile
  profile-errors
  profile-hierarchy
  profile-list
```

Description

This command displays details of all profiles on the device.

Parameter	Description
profile-errors	Displays a list of profiles that are invalid.
profile-hierarchy	Displays the profile hierarchy.
profile-list	Displays the list of profiles of a given type.

Example

The following example shows the output of the `show profile-error` command:

```
Invalid Profiles
-----
Profile                               Error
-----
wlan virtual-ap "AOS-183773-WLAN"    Named VLAN "AOS-183773" does not exist.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show profile-errors

```
show profile-errors
```

Description

Displays the list of invalid user-created profiles.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles. In this example, the VLAN 1000 that is mapped to a virtual-ap that does not exist.

```
(host)[node] #show profile-errors

Invalid Profiles
-----
Profile                Error
-----
wlan virtual-ap "test-vap"  VLAN 1000 does not exist
```

The following are the list of some profile errors:

Error	Description
Named VLAN [named_VLAN] is removed	These errors are displayed if a virtual AP profile is configured with a VLAN that does not exist.
Named VLAN [named_VLAN] is not mapped	
Named VLAN [named_VLAN] is invalid	
VLAN [x] does not exist	
Server group is invalid	This error is displayed if an AAA profile is configured an invalid server group.
User derivation rule is invalid	This error is displayed if a user role in an AAA profile is invalid.
User role is invalid	
controller country code is undefined	These errors are displayed, if your controller is not set to the correct country code or if the country code specified in a WLAN profile does not match the controller's country code.
Country [country_name] does not match controller country [country_name]	

Error	Description
Opmode requires WPA key	This message is displayed if a SSID profile is configured without a WPA key.
WARNING: if weptxkey = [x], wepkey[x] must be set in order to use static WEP	This message is displayed if a SSID profile is configured to use a static WEP and the WEP is not configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Conductor.

show profile-hierarchy

show profile-hierarchy

Description

Displays the profile hierarchy template.

The output of this command shows how profiles relate to each other, and how some higher-level profiles reference other lower-level profiles. The output of this command will vary, depending upon controller configuration and licenses.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show profile-list

```
aaa
airgroupprofile
    airslice-profile
ap
ap-group          ap-name

ble
command-set-profile
dump-collection-profile
est
event-recipe-profile
ha

ids

iot
lc-cluster
license-pool-profile
mgmt-server
pan
policy-domain
rf
scheduler-profile
sso
time-range-profile
wlan
zigbee
```

Description

This command displays details of all profiles on the device.

Parameter	Description
<u>aaa</u>	Displays the list of AAA profiles.
<u>airgroupprofile</u>	Displays the list of configured AirGroup profiles.
<u>airslice-profile</u>	Displays the list of all Air Slice profiles.
<u>ap</u>	Displays the list of AP profiles.
<u>ap-group</u>	Displays the status of AP groups profiles in the controller.
<u>ap-name</u>	Displays the status of AP profiles in the controller.
<u>dump-collection-profile</u>	Displays the list of all dump collection profiles.

Parameter	Description
est	Displays the list of EST profiles.
ha	Displays the list of HA profiles.
ids	Displays the status of all IDS profiles in the controller.
iot	Displays the list of IOT profiles.
lc-cluster	Displays the list of classic controller cluster profiles.
license-pool-profile	Displays the list of license pool profiles.
mgmt-server	Displays all the management configuration profiles in the controller.
pan	Displays the list of all Palo Alto Networks servers profiles.
policy-domain	Displays the list of policy domain profiles.
rf	Displays the status of all radio profiles.
scheduler-profile	Displays the list of scheduler profiles.
sso	Displays the list of all SSO profiles.
time-range-profile	Displays the list of all time range profiles.
wlan	Displays the status of WLAN profiles on the controller.
zigbee	Displays the list of Zigbee profiles.

Example

The following example shows the output of the `aaa dns-query-interval` command:

```
20:4c:03:24:89:18 (config) # a
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show profile-list aaa

```
show profile-list aaa [{alias-group [page | start]} | {authentication [captive-portal | dot1x | mac | stateful-ntlm | wispr]} | {authentication-server [ldap | radius | tacacs | windows]} | {profile} | {rfc-3576-server} | {server-group} | {xml-api}]
```

Description

Displays the list of AAA profiles.

Parameter	Description
alias-group	Lists all alias-groups.
page	Specify the number of items to display
start	Specify the first item to display
authentication	List of aaa authentication profiles.
captive-portal	Captive portal authentication profiles.
dot1x	802.1X authentication profiles.
mac	MAC authentication profiles.
stateful-kerberos	Stateful kerberos authentication profiles.
stateful-ntlm	Stateful-NTLM authentication profiles.
via	VIA authentication profile.
vpn	VPN authentication profiles.
wispr	WISPr authentication profiles.
authentication-server	List of aaa authentication servers
ldap	List of servers using LDAP for AAA authentication.
radius	List of servers using RADIUS for AAA authentication.
tacacs	List of servers using TACACS+ for AAA authentication.
windows	List of Windows servers used for AAA authentication.
profile	Displays the AAA profile details.
page	Specify the number of items to display

Parameter	Description
start	Specify the first item to display
radius modifier	Displays all RADIUS modifier profiles.
page	Specify the number of items to display
start	Specify the first item to display
rfc-3576-server	Displays IP address of RADIUS servers that use RFC 3576 specification to exchange authorization messages.
page	Specify the number of items to display
start	Specify the first item to display
server-group	List of server group used for RADIUS accounting.
page	Specify the number of items to display
start	Specify the first item to display
xml-api server	List of servers configured in an external XML API server.
page	Specify the number of items to display
start	Specify the first item to display

Example

The output of this command shows list of AAA profiles that use captive-portal authentication.

```
(host)[node] # show profile-list aaa authentication captive-portal

Captive Portal Authentication Profile List
-----
Name      References  Profile Status
----      -
default  1
```

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list airgroupprofile

```
show profile-list airgroupprofile {cppm|domain|ipv6|page|service|start} [page | start]
```

Description

Displays the list of configured AirGroup profiles.

Parameter	Description
cppm	Displays all AirGroup ClearPass Policy Manager profiles.
domain	Displays all AirGroup domain profiles.
ipv6	Displays all AirGroup IPv6 profiles.
network	Displays all network profiles.
service	Displays all AirGroup service profiles.
page	Specify the number of items to display.
start	Specify the first item to display.

Example

The output of this command shows a list of AirGroup profiles.

```
(host)[node] (config) # show profile-list airgroupprofile
AirGroup Profile List
-----
Name      References  Profile Status
----      -
default  1
```

Related Commands

Command	Description
airgroupprofile	Configures an AirGroup profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Conductor.

show profile-list airslice-profile

show profile-list airslice-profile [page | start]

Description

Displays the list of all Air Slice profiles.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
profile	Displays all Air Slice profiles.
page	Specify the number of items to display.
start	Specify the first item to display.

Example

The output of this command shows a list of Air Slice profiles.

```
(host) #show profile-list airslice-profile

airslice profile List
-----
Name      References  Profile Status
----      -
default  5
Total:1
```

Related Commands

Command	Description
airslice	This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list ap

```
show profile-list ap [ am-filter-profile | authorization-profile | enet-link-profile | mesh-cluster-profile |  
  mesh-ht-ssid-profile | mesh-radio-profile | regulatory-domain-profile |  
  snmp-profile | snmp-user-profile | system-profile | wired-ap-profile ]
```

Description

Displays the list of AP profiles.

Parameter	Description
am-filter-profile	Display a list of all AM filters.
authorization-profile	Display a list of AP Authorization profiles.
enet-link-profile	Display a list of AP Ethernet link profiles.
lldp	Display Link-layer Discovery Protocol.
mesh-accesslist-profile	Display a list of all mesh accesslist profiles.
mesh-cluster-profile	Display a list of mesh cluster profiles used by mesh nodes.
mesh-ht-ssid-profile	Display a list of mesh high-throughput SSID profiles used by mesh nodes.
mesh-radio-profile	Display a list of mesh radio profiles used by mesh nodes.
multizone-profile	Display a list of all AP MultiZone profile.
provisioning-profile	Display a list of all provisioning profiles.
provisioning-rule	Display a list of all ap provisioning rules.
regulatory-domain-profile	Display a list of AP regulatory profiles.
snmp-profile	Display a list of SNMP profiles.
snmp-user-profile	Display a list of SNMPv3 user profiles.
system-profile	Display a list of AP system profiles.
usb-acl-prof	Display a list of all AP USB ACL profiles.
usb-profile	Display a list of all AP USB profiles.
wifi-uplink-profile	Display a list of all WiFi uplink profiles.

Parameter	Description
wired-ap-profile	Display a list of wired AP profiles.
wired-port-profile	Display a list of all AP wired port profiles.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles.

```
(host)[mynode] # show profile-list aaa authentication captive-portal
Captive Portal Authentication Profile List
-----
Name      References  Profile Status
----      -
default  1
```

Related Commands

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list ap-group

```
show profile-list ap-group
```

Description

Displays the status of AP groups profiles in the controller.

Example

The output of this command shows the status of AP group profiles in the controller.

```
(host)[node] # show profile-list ap-group
AP group List
-----
Name      Profile Status
----      -
default
Total:1
```

Related Commands

Command	Description
ap-group	This command configures an AP group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list ap-name

```
show profile-list ap-name
```

Description

Displays the status of AP profiles in the controller.

Example

The output of this command shows status of AP profiles in the controller.

```
(host)[node] # show profile-list ap-name
AP name List
-----
Name  Profile Status
----  -
Total:0
```

Related Commands

Command	Description
ap-name	This command configures a specific AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list dump-collection-profile

```
show profile-list dump-collection-profile [page<number> start<number>]
```

Description

This command is used to display the list of all dump collection profiles.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The output of this command shows a list of all dump collection profiles,

```
(host)[mynode] #show profile-list dump-collection-profile
Dump collection profile List
-----
Name      References  Profile Status
-----
default   3
Total:1
```

Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list est

show profile-list est profile [page | start]

Description

Displays the list of EST profiles.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
profile	Displays all EST profiles.
page	Specify the number of items to display.
start	Specify the first item to display.

Example

The output of this command shows a list of EST profiles.

```
(host)[node] (config) # #show profile-list est profile

EST Profile List
-----
Name      References  Profile Status
----      -
default  0
Total:1
```

Related Commands

Command	Description
est	This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list iot

```
show profile-list iot radio-profile [page <number>] [start <number>] | transport-profile [page <number>] [start <number>]
```

Description

This command is used to display the list of IOT profiles.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
radio-profile	Displays IoT radio profiles.
transport-profile	Displays IoT transport profiles.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The output of this command shows a list of IoT radio profiles,

```
(host)[mynode] #show profile-list iot radio-profile
IoT Radio Profile List
-----
Name  References  Profile Status
----  -
Total:0
```

Related Commands

Command	Description
iot radio-profile	This command configures an IoT radio profile.
iot Transportprofile	This command configures an IoT transport profile.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list ha

```
show profile-list ha
  group-profile [page | start]
```

Description

Displays the list of HA profiles.

Parameter	Description
group-profile	Lists all HA group information.
page	Specify the number of items to display
start	Specify the first item to display

Example

The output of this command shows list of HA group profile information.

```
(host)[node] # show profile-list ha group-profile
HA group information List
-----
Name  Profile Status
----  -
Total:0
```

Related Commands

Command	Description
ha	This command configures the High Availability:Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list ids

```
show profile-list ids [ap-classification-rule | dos-profile | general-profile |
impersonation-profile |
profile | rap-wml-server-profile | rap-wml-table-profile | rate-thresholds-
profile | signature-matching-profile |
signature-profile | unauthorized-device-profile ]
```

Description

Displays the status of all IDS profiles in the controller.

Parameter	Description
ap-classification-rule	Show all IDS AP classification rule profiles.
dos-profile	Display a list of IDS DoS profiles.
general-profile	Display a list of IDS general profiles.
impersonation-profile	Display a list of IDS impersonation profiles.
profile	Display a list of IDS profiles.
rap-wml-server-profile	Show all IDS RAP WML server profiles.
rap-wml-table-profile	Show all IDS RAP WML table profiles.
rate-thresholds-profile	Display a list of IDS rate threshold profiles.
signature-matching-profile	Display a list of IDS signature-matching profiles.
signature-profile	Display a list of IDS signature profiles.
unauthorized-device-profile	Display a list of IDS unauthorized device profiles.

Example

The output of this command shows a list of all IDS DoS profiles.

```
(host)[node] # show profile-list ids dos-profile
IDS Denial Of Service Profile List
-----
Name                References  Profile Status
----                -
default             1
ids-dos-disabled    1          Predefined
ids-dos-high-setting 1          Predefined
ids-dos-low-setting  1          Predefined
```

```
ids-dos-medium-setting 1          Predefined
Total:5
```

Related Commands

Command	Description
ids general-profile	This command configures an IDS general profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list lc-cluster

```
show profile-list lc-cluster
  group-profile [page | start]
```

Description

Displays the list of classic controller cluster profiles.

Parameter	Description
group-profile	Lists all controller cluster profiles.
page	Specify the number of items to display.
start	Specify the first item to display.

Example

The output of this command shows a list of all controller cluster profiles.

```
(host)[node]# show profile-list lc-cluster group-profile
Classic controller Cluster Profile List
-----
Name      Profile Status
----      -
LC-west
Total:1
```

Related Commands

Command	Description
lc-cluster group-profile	This command is used to configure the cluster group profile in the Mobility Conductor.
lc-cluster group-membership	Configure the group-membership in each node. This command is used to enable the cluster membership on the managed devices.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list license-pool-profile

show profile-list license-pool-profile [page | start]

Description

Displays the list of license pool profiles.

Parameter	Description
page	Specify the number of items to display.
start	Specify the first item to display.

Example

The output of this command shows a list of all licensing pools.

```
(host)[node] (config) #show profile-list license-pool-profile
License pool profile List
-----
Name           References  Profile Status
----           -
/md/dev        2
/md/Sunnyvale  1
/md/testpool   0
/md/Testpool2  0
```

Related Commands

Command	Description
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list mgmt-server

```
show profile-list mgmt-server {profile <profile_name>} [page <number>] [start <number>]
```

Description

Displays all the Mgmt Config profiles in the controller.

Parameter	Description
mgmt-server {profile <profile_name>}	Specifies the name of the management server profile.
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

The output of this command shows the management server profiles in the controller.

```
(host) (config) #show profile-list mgmt-server profile
Mgmt Config profile List
-----
Name           References  Profile Status
----           -
default-ale    0           Predefined (editable)
default-amp    0           Predefined (editable)
Total:2
```

Related Commands

Command	Description
mgmt-user	This command configures an administrative user.
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list pan profile

```
show profile-list pan profile
```

Description

This command is used to display the list of all Palo Alto Networks servers profiles.

Example

The output of this command shows a list of all time range profiles,

```
[host](mynode) #show profile-list pan profile
Palo Alto Networks Servers Profile List
-----
Name      References  Profile Status
----      -
default  1
Total:1
```

Related Commands

Command	Description
pan-active-profile	This command makes a Palo Alto Network profile active from a set of profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list policy-domain

```
show profile-list policy domain
  group-profile
    page <page>
    start <start>
```

Description

Displays the list of policy domain profiles.

Parameter	Description
group-profile	Displays all policy domain profiles.
page <page>	Specify the number of items to display.
start <start>	Specify the index of first item to display.

Example

The output of this command shows the list of policy domain profiles.

```
(host) # show profile-list policy-domain group-profile

Policy Domain Profile List
-----
Name  Profile Status
----  -
Total:0
```

Related Commands

Command	Description
policy-domain	This command configures a policy domain profile to apply role-based ACL for users present in different controllers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list rf

```
show profile-list rf [ am-scan-profile | arm-profile | dot11-60GHz-radio-profile |  
dot11-6GHz-radio-profile | dot11a-radio-profile | dot11a-secondary-radio-  
profile |  
dot11g-radio-profile | event-thresholds-profile | ht-radio-profile |  
optimization-profile | spectrum-profile ]
```

Description

Displays the status of all radio profiles.

Parameter	Description
am-scan-profile	Display AM scanning profiles.
arm-profile	Display details of Adaptive Radio Management (ARM) Profiles.
dot11-60GHz-radio-profile	Display details of AP radio settings for the 60GHz frequency band.
dot11-6GHz-radio-profile	Display details of AP radio settings for the 6GHz frequency band.
dot11a-radio-profile	Display details of AP radio settings for the 5GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
dot11a-secondary-radio-profile	Display details of secondary AP radio settings for the 5GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
dot11g-radio-profile	Display details of AP radio settings for the 2.4 GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
event-thresholds-profile	Display details of events thresholds profile.
ht-radio-profile	Display details of high-throughput AP radio settings
optimization-profile	Display details of the RF optimization profile
spectrum-profile	Display details of the spectrum profile

Example

The output of this command shows status of ARM profile.


```
(host) # show profile-list rf arm-profile

Adaptive Radio Management (ARM) profile List
-----
Name      References  Profile Status
-----
default   2
Total:1
```

Related Commands

Command	Description
rf arm-profile	This command configures the Adaptive Radio Management (ARM) profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list scheduler-profile

show profile-list scheduler-profile [page | start]

Description

Displays the list of scheduler profiles.

Parameter	Description
page	Specify the number of items to display
start	Specify the first item to display

Example

The output of this command shows a list of scheduler profiles.

```
(host)[node] (config) # show profile-list scheduler-profile
scheduler profile List
-----
Name       References  Profile Status
----       -
default    2
Total:1
```

Related Commands

Command	Description
scheduler-profile	Define a schedule profile that associates priorities to four uplink queues.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list sso idp-profile

```
show profile-list sso idp-profile
```

Description

This command is used to display the list of all SSO profiles.

Example

The output of this command shows a list of all SSO profiles,

```
(host)[mynode] #show profile-list sso idp-profile
SSO Profile List
-----
Name   References  Profile Status
-----
Total:0
```

Related Commands

Command	Description
sso idp-profile	This command configures an IDP-SSO profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list time-range-profile

```
show profile-list time-range-profile [page | start]
```

Description

This command is used to display the list of all time range profiles.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The output of this command shows a list of all all time range profiles.

```
Time range profile List
-----
Name  References  Profile Status
----  -
Total:0
```

Related Commands

Command	Description
time-range	This command configures time ranges. You can use time ranges when configuring session ACLs. Once you configure a time range, you can use it in multiple session ACLs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list wlan

```
show profile-list wlan
  6ghz-rrm-ie-profile
  anyspot-profile
  bcn-rpt-req-profile
  client-wlan-profile
  dot11k-profile
  dot11r-profile
  edca-parameters-profile
  he-ssid-profile
  hotspot
  ht-ssid-profile
  mu-edca-parameters-profile
  rrm-ie-profile
  ssid-profile
  traffic-management-profile
  tsm-req-profile
  virtual-ap
  wmm-traffic-management-profile
```

Description

Displays the status of WLAN profiles on the controller.

Parameter	Description
6ghz-rrm-ie-profile	Show a list of all RRM IE profiles for 6GHz
anyspot-profile	Shows a list of all anyspot profiles
bcn-rpt-req-profile	Shows a list of all Beacon Report Request profiles
client-wlan-profile	Shows a list of all client WLAN profiles
dot11r-profile	Shows a list of all 802.11r profiles
dot11k-profile	Show a list of all 802.11K profiles
edca-parameters-profile	Show a list of all enhanced distributed channel access (EDCA) profile for APs or for clients (stations)
he-ssid-profile	Show a list of all high-efficiency SSID profiles
hotspot	Hotspot/Passpoint configuration settings
advertisement-profile	Shows a list of all Advertisement profile
angp-3gpp-nwk-profile	Shows a list of all ANQP 3GPP Cellular Network profiles

Parameter	Description
anqp-domain-name-profile	Shows a list of all ANQP Domain Name profiles
anqp-ip-addr-avail-profile	Shows a list of all ANQP IP Address Availability profiles
anqp-nai-realm-profile	Shows a list of all ANQP NAI Realm profiles
anqp-nwk-auth-profile	Shows a list of all ANQP Network Authentication profiles
anqp-roam-cons-profile	Shows a list of all ANQP Roaming Consortium profiles
anqp-venue-name-profile	Shows a list of all ANQP Venue Name profiles
h2qp-conn-capability-profile	Shows a list of all H2QP Connection Capability profiles
h2qp-op-cl-profile	Shows a list of all H2QP Operating Class Indication profiles
h2qp-operator-friendly-profile	Shows a list of all H2QP Operator Friendly Name profiles
h2qp-wan-metrics-profile	Shows a list of all H2QP WAN Metrics profiles
hs2-profile	Shows a list of all Hotspot 2.0 profiles
ht-ssid-profile	Show a list of all high-throughput SSID profiles
mu-edca-parameters-profile	Show a list of all MU EDCA parameters profiles
rrm-ie-profile	Shows a list of all Radio Resource Management Information Element (RRM IE) profiles
ssid-profile	Show a list of all SSID profiles.
traffic-management-profile	Show a list of all traffic management profiles
tsm-req-profile	Show a list of all Transmit Stream/Category Measurement (TSM) request profiles
virtual-ap	Show a list of all the virtual AP profiles
wmm-traffic-management-profile	Show a list of all WMM traffic management profiles

Example

The output of this command shows that the controller has a single ARM profile, "default".

```
(host)[mynode] # show profile-list wlan anysot-profile

Anysot profile List
-----
```


Name	References	Profile Status
----	-----	-----

Total:0

Related Commands

Command	Description
wlan ssid-profile	This command configures an SSID profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show profile-list zigbee

```
show profile-list zigbee
  service-profile
  socket-device-profile
  socket-inbound-profile
  socket-outbound-profile
```

Description

This command is used to display the list of zigbee profiles.

Parameter	Description
service-profile	Display all ZigBee service profiles.
socket-device-profile	Display all Zigbee socket device profiles.
socket-inbound-profile	Display all Zigbee socket inbound profiles.
socket-outbound-profile	Display all Zigbee socket outbound profiles.

Example

```
(host) [node] # show profile-list zigbee service-profile

ZigBee Service Profile List
-----
Name  References  Profile Status
----  -
Total:0
```

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on the Mobility Conductor.

show provisioning

```
show provisioning
  rule info
  params
  ap-list
```

Description

This command displays the AP provisioning details that are described in the following table:

Parameter	Description
<rule-info>	Displays detailed information about the AP auto-provisioning rules.
<params>	Displays the list of parameters and the values used to provision the APs.
<ap-list>	Displays the list of all APs that are in queue to be provisioned by the admin.

Example

The following example shows the output of the `show-provisioning` command:

```
provisioning-ap-list    The APs that are being provisioned
provisioning-params    Show AP provisioning parameters
provisioning-rule-info  AP auto provisioning rule
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show provisioning-ap-list

show provisioning-ap-list

Description

Displays the list of all APs that are in queue to be provisioned by the admin.

Example

```
(host) [mynode]# show provisioning-ap-list
Access Points Provisioning List
-----
Current IP      AP Name  AP Group  Location name  SNMP sysLocation  AP Type
Serial #      AP State
-----
-----
191.191.191.253  ap-215  default   N/A            N/A                215
CK0223282      -
Total APs:1
```

Related Commands

Command	Description
ap provisioning-profile	This command defines a provisioning profile for an AP or group of APs.
provision-ap	This command provisions or re-provisions an AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on the Mobility Conductor.

show provisioning-params

show provisioning-params

Description

Displays the list of parameters and the values used to provision the APs.

Example

The output of this command shows list of all provisioning parameters and their values.

```
(host) [mynode]# show provisioning-params
AP provisioning
-----
Parameter                                     Value
-----
AP Name                                       N/A
AP Group                                       default
Location name                               N/A
SNMP sysLocation                             N/A
Master/Conductor                             N/A
Gateway                                       N/A
IPv6 Gateway                                 N/A
Netmask                                       N/A
IP Addr                                       N/A
IPv6 Addr                                     N/A
IPv6 Prefix                                  64
DNS IP                                        N/A
DNS IPv6                                      N/A
Domain Name                                  N/A
Server Name                                  N/A
Server IP                                    N/A
Antenna gain for 802.11a                     N/A
Antenna gain for 802.11g                     N/A
Use external antenna                         No
Antenna for 802.11a                          both
Antenna for 802.11g                          both
PKCS12 PASSPHRASE                           N/A
Single chain mode for Radio 0                 0
Single chain mode for Radio 1                 0
External antenna polarization for 5GHz Radio  0
External antenna polarization for 2.4GHz Radio 0
TrustAnchor                                  N/A
IKE PSK                                       N/A
ikepsk-hex-based                             No
PAP User Name                                N/A
PAP Password                                  N/A
PPPOE User Name                              N/A
PPPOE Password                               N/A
PPPOE Service Name                           N/A
```

```

PPPOE CHAP Secret N/A
USB User Name N/A
USB Password N/A
USB Device Type none
USB CSR-Key Storage No
USB Device Identifier N/A
USB Dial String N/A
USB Initialization String N/A
USB TTY device data path N/A
USB TTY device control path N/A
USB modeswitch parameters N/A
Uplink VLAN 0
Remote AP No
OCSP Default N/A
certificate DN N/A
Link Priority Ethernet 0
Link Priority Cellular 0
Cellular modem network preference auto
USB power mode auto
AP POE Power optimization false
AP2xx prestandard POE detection Disabled
Mesh Role none
Installation default
Latitude N/A
Longitude N/A
Altitude N/A
Antenna bearing for 802.11a N/A
Antenna bearing for 802.11g N/A
Antenna tilt angle for 802.11a N/A
Antenna tilt angle for 802.11g N/A
Username of AP so that AP can authenticate to 802.1x using PEAP N/A
Password of AP so that AP can authenticate to 802.1x using PEAP N/A
Enable AP to 802.1x using EAP-TLS Disabled
Enable AP to use factory certificates when doing 802.1x EAP-TLS Disabled
AP dot1x EAP-TLS username suffix Disabled
AP dot1x EAP-TLS username suffix domain aruba.ap
Mesh SAE sae-disable

```

Related Commands

Command	Description
ap provisioning-profile	This command defines a provisioning profile for an AP or group of APs.
provision-ap	This command provisions or reprovisions an AP.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.4.0.0	The output of the <code>show provisioning-params</code> command was modified to include the following parameters: <ul style="list-style-type: none"> ■ <code>AP dot1x EAP-TLS username suffix</code> ■ <code>AP dot1x EAP-TLS username suffix domain</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show provisioning-rule-info

```
show provisioning-rule-info [record <rule-name>|summary]
```

Description

This command displays detailed information about the AP auto-provisioning rules.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
record <rule-name>	Display information about the MAC address of the AP that the auto-provisioning rule is applied to, along with the provisioning time, LMS IP of the AP, and auto-provisioning state of the AP.
summary	Display information about the auto-provision rule of each AP in ascending order of the rule-priority, the hit times of that rule, as well as the success and failure count of the rules.

Examples

The following example displays the summary of the auto-provisioning rules.

```
(host) [mm] #show provisioning-rule-info summary

Auto provision Rule Info
-----
Rule Name  Priority  Hit times  Success count
-----
ap324      1         0          0
ip36       3         0          0
network    5         0          0
ip46       7         0          0
The following example displays information on each auto-provisioning rule and
the associated AP.
(host) [mm] #show provisioning-rule-info record ap324
Auto provision Rule Info
-----
Rule Name  Priority  Hit times  Success count
-----
ap324      1         1          1

Auto provision Rule Record
-----
```

```

AP MAC          Provision Time      LMS
-----          -
40:e3:d6:cd:82:34  2018-07-01 13:55:06  10.65.46.203

```

The output of this command includes the following information:

Parameter	Description
Rule Name	Indicates the name of the auto-provisioning rule that is applied to the AP.
Priority	Indicates the priority level of the auto-provisioning rule. The rules are listed in ascending order of the priority level.
Hit times	Indicates the hit times of the auto-provisioning rule.
Success count	Indicates the success count of the auto-provisioning rule.
AP MAC	Indicates the MAC address of the AP that the auto-provisioning rule is applied to.
Provision Time	Indicates the date and time when the auto-provisioning rule is applied to the AP.
LMS	Indicates the LMS IP of the AP that the auto-provisioning rule is applied to.

Related Commands

Command	Description
show ap provisioning-profile	This command shows information for AP provisioning profiles.
ap provisioning-rule	This command defines the conditions to select a group of APs and the subsequent actions to provision the APs.

Command History

Version	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show rap-wml

```
show rap-wml [cache <server-name> | servers | wired-mac <bssid>]
```

Description

Displays the name and attributes of a MySQL database or a MySQL server.

Parameter	Description
cache <server-name>	Displays the cache of all look-ups for a database server.
servers	Displays the database server state.
wired-mac <bssid>	Displays the wired MAC discovered on traffic through the AP.

Example

The output of this command shows status of all database servers.

```
(host) [mynode] #show rap-wml servers

WML DB Servers
-----
name ip type user password db-name cache ageout(sec) in-service
-----
WML DB Tables
-----
server db table column timestamp-column lookup-time(sec) delimiter
query-count
-----
Mesh SAE sae-default
```

Related Commands

Command	Description
ids rap-wml-server-profile	This command configures an IDS remote AP WML (MSSQL or MySQL) server profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on the Mobility Conductor.

show references aaa alias-group

```
show references aaa
  alias-group <ag_name>
  [page <page>] [start <start>]
```

Description

Shows AAA profile references to an alias group.

Parameter	Description
alias-group <ag_name>	Shows the references to an Alias group.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show the references to an alias group.

```
(host)[mynode] #show references aaa alias-group alias1
```

Related Commands

Command	Description
aaa alias-group	Configures an AAA alias with set of VLAN derivation rules that could speed up user rule derivation processing for deployments with a very large number of user derivation rules.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa authentication

```
show references aaa authentication
  captive-portal {default | <profile-name>}
  dot1x {default | <profile-name>}
  mac {default | <profile-name>}
  mgmt
  stateful-dot1x
  stateful-kerberos {default | <profile-name>}
  stateful-ntlm {default | <profile-name>}
  via
    auth-profile {default | <profile-name>}
    connection-profile {default | <profile-name>}
    global-config
    web-auth <default>
  vpn {default | <profile-name>}
  wired
  wispr {default | <profile-name>}
  [page <page>] [start <start>]
```

Description

This command shows AAA profile references.

Parameter	Description	Default
captive-portal <profile-name>	Shows the number of references to a captive-portal profile.	default
dot1x <profile-name>	Shows the number of references to a 802.1X authentication profile.	default
mac <profile-name>	Shows the number of references to a MAC authentication profile.	default
mgmt	Shows the number of references to a management authentication profile.	
stateful-dot1x <profile-name>	Shows the number of references to the stateful 802.1X authentication profile.	default
stateful-kerberos <profile-name>	Shows references to a Stateful Kerberos authentication profile.	default

Parameter	Description	Default
<code>stateful-ntlm <profile-name></code>	Shows the number of references to the specified stateful NTLM authentication profile.	default
<code>via</code>	Shows the number of references to VIA.	
<code>auth-profile <profile-name>}</code>	Shows references to a VIA authentication profile.	default
<code>connection-profile <profile-name></code>	Shows references to a VIA connection profile.	default
<code>global-config</code>	Shows references to the VIA global configuration.	
<code>web-auth <default></code>	Shows references to a VIA web authentication.	default
<code>vpn <profile-name></code>	Shows the number of references to VPN authentication.	default
<code>wired</code>	Shows the number of references to wired authentication.	
<code>wispr <profile-name></code>	Shows the number of references to the specified WISPr authentication profile.	default
<code>page <page></code>	Include this optional parameter to limit output of this command to the specified number of items.	
<code>start <start></code>	Include this optional parameter to start displaying the output of this command at the specified index number.	

Example

Use this command to show where a specified AAA profile has been applied. The output of the example shown here indicates that the aaa profile **default-dot1x** contains a single reference to the 802.1X authentication profile **default**.

```
(host)[mynode] #show references aaa authentication dot1x default
```

```

References to 802.1X Authentication Profile "default"
-----
Referrer                                     Count
-----
aaa profile "default-dot1x" authentication-dot1x  1
Total References:1

```

Related Commands

Command	Description
aaa authentication captive-portal	Configures a Captive Portal authentication profile.
aaa authentication dot1x	Configures the 802.1X authentication profile.
aaa authentication mac	Configures the MAC authentication profile.
aaa authentication mgmt	Configures authentication for administrative users.
aaa authentication stateful-dot1x	Configures 802.1X authentication for clients on non-Aruba APs.
aaa authentication stateful-kerberos	Configures stateful Kerberos authentication.
aaa authentication stateful-ntlm	Configures stateful NT LAN Manager (NTLM) authentication.
aaa authentication via auth-profile	Configures the VIA authentication profile.
aaa authentication via connection-profile	Configures the VIA connection profile.
aaa authentication via global-config	Allows you to enable SSL fallback mode.
aaa authentication via web-auth	Creates a VIA web authentication profile.
aaa authentication vpn	This command configures VPN authentication settings.
aaa authentication wired	Configures authentication for a client device that is directly connected to a port on the managed device.
aaa authentication wispr	Configures WISPr authentication with WISPr RADIUS server of an ISP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa authentication-server

```
show references aaa authentication-server
  ldap <ldap_server_name>
  radius <rad_server_name>
  tacacs <tacacs_server_name>
  windows <windows_server_name>
  [page <page>] [start <start>]
```

Description

This command displays information about AAA authentication servers.

Parameter	Description
ldap <ldap-server-name>	Show the number of server groups that include references to the specified LDAP server.
radius <rad_server_name>	Show the number of server groups that include references to the specified RADIUS server.
tacacs <tacacs_server_name>	Show the number of server groups that include references to the specified TACACS server.
windows <windows_server_name>	Show the number of server groups that include references to the specified Windows server.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to show the AAA server groups that include references to the specified server. The example below shows that two server groups, **default** and **rad**, each include a single reference to the RADIUS server **rad01**.

```
(host)[mynode] #show references aaa authentication-server radius rad01

References to RADIUS Server "rad01"
-----
Referrer                                Count
-----                                -
aaa server-group "default" server_group  1
aaa server-group "rad" server_group      1
Total References:2
```

Related Commands

Command	Description
aaa authentication-server ldap	Configures an LDAP server.
aaa authentication-server radius	Configures a RADIUS server.
aaa authentication-server tacacs	Configures a TACACS+ server.
aaa authentication-server windows	Configures a windows server for stateful-NTLM authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa password-policy

```
show references aaa password-policy mgmt
```

Description

This command shows the password policy for locally configured management users.

Parameter	Description
mgmt	Shows references to the Management Password Policy.

Example

Execute the following command to show the password policy for locally configured management users.

```
(host)[mynode] #show references aaa password-policy mgmt
```

Related Commands

Command	Description
aaa password-policy mgmt	Defines a policy for creating management user passwords.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa profile

show references aaa profile <profile-name>

Description

This command shows references to an AAA Profile.

Parameter	Description
profile <profile-name>	Name of an AAA profile for which you want to view references.

Example

Issue this command to show the wlan virtual AP profiles that include references to the specified AAA profile. The example below shows that seven different virtual AP profiles include a single reference to the AAA profile **default**.

```
(host)[mynode] #References to AAA Profile "default"
-----
Referrer                                     Count
-----
wlan virtual-ap "1.0.0_corporateHQ-wpa2" aaa-profile 1
wlan virtual-ap "110.0_corporateHQ-wpa2" aaa-profile 1
wlan virtual-ap "default" aaa-profile 1
wlan virtual-ap "corporateHQ-vocera" aaa-profile 1
wlan virtual-ap "corporateHQ-voip-wpa2" aaa-profile 1
wlan virtual-ap "Test123" aaa-profile 1
wlan virtual-ap "branch12" aaa-profile 1
Total References:7
```

Related Commands

Command	Description
aaa profile	This command configures the authentication for a WLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa radius

```
show references aaa
  radius modifier <rad_modifier_name>
  [page <page>] [start <start>]
```

Description

This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Parameter	Description
<code>radius modifier <rad_modifier_name></code>	Shows references to a RADIUS modifier profile.
<code>page <page></code>	Include this parameter to limit output of this command to the specified number of items.
<code>start <start></code>	Include this parameter to start displaying the output of this command at the specified index number

Example

The following is an example to execute the `show references aaa radius modifier` command:

```
(host) [mynode] #show references aaa radius modifier RADIUSProfile1
```

Related Commands

Command	Description
aaa radius modifier	Configures the RADIUS modifier profile to customize the attributes that are included, excluded, and modified in the RADIUS request before it is sent to the authentication server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa radius-attributes

```
show references aaa
  radius-attributes <node-path>
```

Description

This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Parameter	Description
radius-attributes	Displays references to RADIUS attributes.
<node-path>	Displays the path of the configuration node.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example to execute the `show references aaa radius-attributes` command:

```
(host) [mynode] #show references aaa radius-attributes HW-Cluster-1
```

Related Commands

Command	Description
aaa radius-attributes	Configures the RADIUS attributes to statically configure values to be included in RADIUS Access- Requests and Accounting-Requests.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa rfc-3576-server

```
show references aaa
  rfc-3576-server <server_ip>
  [page <page>] [start <start>]
```

Description

This command shows information about the configuration profiles that reference a specific RFC 3576 server.

Parameter	Description
rfc-3576-server <server_ip>	IP address of an RFC-3576 server.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number

Example

This first example shows that the **default** AAA profile and the AirGroup ClearPass Policy Manager-server AAA profile reference an RFC 3567 Server with the IP address 10.1.1.41.

```
(host)[mynode] #show references aaa rfc-3576-server 10.1.1.41
References to RFC 3576 Server "10.1.1.41"
-----
Referrer                                     Count
-----
aaa profile "default" rfc-3576-server       1
airgroup cppm-server aaa rfc-3576-server    1
Total References:2
```

Related Commands

Command	Description
aaa rfc-3576-server	Define RFC 3576 server profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa server-group

```
show references aaa server-group
  <sg_name>
  [page <page>][start <start>]
```

Description

This command shows references to a server group.

Parameter	Description
<sg_name>	Name of the server group for which you want to show references
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to display a list of AAA profiles that include references to the specified server group.

```
(host)[mynode] #show references aaa server-group default

References to Server Group "default"
-----
Referrer                                     Count
-----
aaa profile "aircorp-office-ssid" mac-server-group 1
aaa profile "amigopod-guest" mac-server-group 1
aaa profile "default" mac-server-group 1
aaa profile "default-airwave-office" mac-server-group 1
aaa profile "defaultcorporate" mac-server-group 1
aaa profile "defaultcorporate-no-okc" mac-server-group 1
aaa profile "defaultcorporate-okc" mac-server-group 1
aaa profile "default-dot1x" mac-server-group 1
aaa profile "default-India" mac-server-group 1
aaa profile "default-india-hotel" mac-server-group 1
aaa profile "default-India-split" mac-server-group 1
aaa profile "voip-psk" mac-server-group 1
aaa profile "default-dot1x-psk" mac-server-group 1
aaa profile "default-mac-auth" mac-server-group 1
aaa profile "default-open" mac-server-group 1
aaa profile "default-xml-api" mac-server-group 1
Total References:16
```

Related Commands

Command	Description
aaa server-group	Allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aaa xml-api server

```
show references aaa
  xml-api server <server-id>
  [page <page>][start <start>]
```

Description

This command shows references to an XML API Server.

Parameter	Description
xml-api server <server-id>	Shows references to an XML API Server. Specify the IP address of the XML-API server.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references to the specified XML-API server.

```
(host) [mynode] #show references aaa xml-api server 191.1.2.1
```

Related Commands

Command	Description
aaa xml-api	Configures an external XML API server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references activate

```
show references activate  
[page <page>] [start <start>]
```

Description

This command displays Activate service whitelist/allowlist profile references.

Parameter	Description
activate	Name of the activate profile for which you want to show references.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of profiles that include references to the activate profile.

```
(host) [mynode] #show references activate  
References to activate  
-----  
Referrer  Count  
-----  ----  
Total References:0
```

Related Commands

Command	Description
activate	Synchronizes a managed device whitelist/allowlist remote AP whitelist/allowlist on Mobility Conductor with the Activate whitelist/allowlist database.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references airgroup

```
show references airgroup
  cppm-server aaa
  [page <page>] [start <start>]
```

Description

This command displays information about AAA authentication servers.

Parameter	Description
cppm-server	Specifies the ClearPass Policy Server information.
aaa	Specifies the AAA parameters for AirGroup.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show the AAA server groups that include references to the AirGroup.

```
(host)[mynode] #show reference airgroup
References to Airgroup AAA profile
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Command	Description
airgroup	configures AirGroup settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references airgroupprofile

```
show references airgroupprofile
  activate
  cppm <airgroup-cppm-name>
  domain <airgroup-domain-name>
  ipv6 <ipv6-profile-name>
  network <network-profile-name>
  service <service-name>
  [page <page>] [start <start>]
```

Description

This command shows the references to the AirGroup profile information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Parameter	Description
activate	Displays references to the active AirGroup profile.
cppm <airgroup-cppm-name>	Displays references to the AirGroup ClearPass Policy Manager profile.
domain <airgroup-domain-name>	Displays references to an AirGroup domain profile.
ipv6 <ipv6-profile-name>	Displays references to the AirGroup IPv6 profile.
network <network-profile-name>	Displays references to the network profile.
service <service-name>	Displays references to the AirGroup service profile. By default, the following services are available: <ul style="list-style-type: none">■ default-airplay■ default-airprint■ default-allowall■ default-amazontv■ default-dial■ default-dlna-media■ default-dlna-print■ default-googlecast■ default-itunes■ default-remotemgmt■ default-sharing
<profile-name>	Configures an AirGroup profile.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.

Parameter	Description
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show the AirGroup domain profiles.

```
(host)[mynode] ##show references airgroupprofile cppm test
```

Related Commands

Command	Description
airgroupprofile	Configures AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references airmatch

```
show references airmatch
  profile
  [page <page>] [start <start>]
```

Description

The `show references profile` command displays profile references. No other profiles reference the AirMatch profile, so the output of this always displays a reference count of 0.

Parameter	Description
<code>profile</code>	Shows references to the AirMatch profile
<code>page <page></code>	Include this parameter to limit output of the <code>show references</code> command to the specified number of items.
<code>start <start></code>	Include this parameter to start displaying the output of the <code>show references</code> command at the specified index number.

Example

The `show references <profile>` command displays a list of profiles that include references to the selected profile. No other profiles reference the AirMatch profile, so this table always displays a reference count of 0.

```
(host) [mynode] #show references airmatch profile
References to AirMatch
-----
Referrer  Count
-----  ----
Total References:0
```

Related Commands

Command	Description
airmatch profile	Configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references airslice-profile

```
show references airslice-profile <profile name>
    [page <page>] [start <start>]
```

Description

This command displays references to an airslice profile.

Parameter	Description
<profile name>	Specify profile name.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode] #show references airslice-profile default

References to airslice profile "default"
-----
Referrer                                     Count
-----
ap-group "$(touch /flash/config/proof1)" airslice-profile 1
ap-group "default" airslice-profile 1
ap-group "NoAuthApGroup" airslice-profile 1
Total References:3
```

Related Commands

Command	Description
airslice	configures AirSlice settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ap

```
show references ap
  am-filter-profile {default | <profile-name>}
  authorization-profile {default | <profile-name>}
  deploy-profile {page | start}
  enet-link-profile {default | <profile-name>}
  general-profile
  lldp
    med-network-policy-profile
      {default | <profile-name>}
    profile
  mesh-accesslist-profile {default | <profile-name>}
  mesh-cluster-profile {default | <profile-name>}
  mesh-ht-ssid-profile {default | <profile-name>}
  mesh-radio-profile {default | <profile-name>}
  multizone-profile {default | <profile-name>}
  provisioning-profile {default | <profile-name>}
  provisioning-rule {default | <profile-name>}
  provisioning-rules
  regulatory-domain-profile {default | <profile-name>}
  spectrum local-overridead
  system-profile {default | <profile-name>}
  usb-acl-prof {default | <profile-name>}
  usb-profile {default | <profile-name>}
  wifi-uplink-profile {default | <profile-name>}
  wired-ap-profile {default | <profile-name>}
  wired-port-profile
  [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP profile.

Parameter	Description	Default
am-filter-profile <profile-name>	Shows references to an AM filter.	default
authorization-profile <profile-name>	Shows references to an AP Authorization profile.	default
deploy-profile	Show references to the AP deploy-profile.	
enet-link-profile <profile-name>	Shows AP groups that include a references to this Ethernet link profile.	default

Parameter	Description	Default
general-profile	Shows references to the ap general-profile.	
lldp	Shows references to the Link-layer Discovery Protocol profile.	
mesh-accesslist-profile <profile-name>	Shows references to the mesh accesslist profile.	default
med-network-policy-profile <profile-name>	Shows references to LLDP-MED Network Policy profile of an AP.	
profile	Shows references to an AP LLDP profile.	
mesh-cluster-profile <profile-name>	Shows AP groups that include a references to this mesh cluster profile.	default
mesh-ht-ssid-profile <profile-name>	Shows AP groups that include a references to this mesh high-throughput SSID profile.	default
mesh-radio-profile <profile-name>	Shows AP groups that include a references to this mesh radio profile.	default
multizone <profile-name>	Shows references to an AP MultiZone profile.	default
provisioning-profile <profile-name>	Shows references to a Provisioning profile.	default
provisioning-rule	Shows references to an ap provisioning rule.	default
provisioning-rules	Shows references to the ap provisioning rules.	
regulatory-domain-profile <profile-name>	Shows AP groups that include a references to this regulatory domain profile.	default
spectrum local-override	Shows references to the Spectrum Local Override Profile.	
system-profile <profile-name>	Shows AP groups that include a references to this system profile.	default

Parameter	Description	Default
usb-acl-prof <profile-name>	Shows references to an AP USB ACL profile.	
usb-profile <profile-name>	Shows references to an AP USB profile.	
wifi-uplink-profile <profile-name>	Shows references to a WiFi uplink profile.	
wired-ap-profile <profile-name>	Shows AP groups that include a references to this wired AP profile.	default
wired-port-profile <profile-name>	Shows references to an AP wired port profile	default
page <page>	Include this optional parameter to limit output of this command to the specified number of items.	
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.	

Example

The example below shows that 10 different AP groups include links to the AP Ethernet link profile **Default**. These 10 AP groups reference the **Default** Ethernet link profile for both their Ethernet 0 and Ethernet 1 interfaces, for a total of 20 references altogether.

```
(host)[mynode] #show references ap enet-link-profile default

References to AP Ethernet Link profile "default"
-----
Referrer                                     Count
-----
ap-group "10.0.0" enet0-profile             1
ap-group "10.0.0" enet1-profile             1
ap-group "corp" enet0-profile               1
ap-group "corp" enet1-profile               1
ap-group "Corp_AM_Ch1" enet0-profile        1
ap-group "Corp_AM_Ch1" enet1-profile        1
ap-group "Corp_AM_Ch6" enet0-profile        1
ap-group "Corp_AM_Ch6" enet1-profile        1
ap-group "corpTest" enet0-profile           1
ap-group "corpTest" enet1-profile           1
ap-group "default" enet0-profile            1
```

```

ap-group "default" enet1-profile 1
ap-group "India_Local" enet0-profile 1
ap-group "India_Local" enet1-profile 1
ap-group "ops" enet0-profile 1
ap-group "ops" enet1-profile 1
ap-group "voip-test" enet0-profile 1
ap-group "voip-test" enet1-profile 1
ap-group "voip-test-nokia" enet0-profile 1
ap-group "voip-test-nokia" enet1-profile 1
Total References:20

```

Related Commands

Command	Description
ap am-filter-profile	Configures an AM filter.
ap authorization-profile	Defines a temporary configuration profile for remote APs that are not yet authorized on the network.
ap deploy-profile	Configures an AP deployment profile.
ap enet-link-profile	Configures an AP Ethernet link profile.
ap general-profile	Configures the general profile of an AP.
ap lldp profile	Defines an LLDP profile that specifies the type-length-value (TLV) elements to be sent in LLDP PDUs.
ap lldp med-network-policy-profile	Defines an LLDP MED network policy profile that defines DSCP values and L2 priority levels for a voice or video application.
ap mesh-cluster-profile	Configures a mesh cluster profile used by mesh nodes.
ap mesh-ht-ssid-profile	Configures a mesh high-throughput SSID profile used by mesh nodes.
ap mesh-radio-profile	Configures a mesh radio profile used by mesh nodes.
ap multizone-profile	Attaches the profile to ap-group or ap-name.
ap provisioning-profile	Defines a provisioning profile for an AP or group of APs.
ap regulatory-domain-profile	Configures an AP regulatory domain profile.
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
ap system-profile	Configures an AP system profile.

Command	Description
ap wired-ap-profile	Configures a wired AP profile.
ap wired-port-profile	Configures a wired port profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The <code>ap deploy-profile</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ap-group

```
show references
  ap-group {default | <profile-name>}
  [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP-group profile.

Parameter	Description	Default
ap-group <profile-name>	Shows references to an AP-group profile.	default

Example

The following is an example for execution of the `show references ap-group` command:

```
(host) [mynode] #show references ap-group LeftWing
```

Related Commands

Command	Description
ap-group	Configures an AP group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Conductor

show references ap-lacp-striping-ip

```
show references
  ap-lacp-striping-ip
  [page <page>] [start <start>]
```

Description

This command shows the references to the AP LACP LMS map information.

Parameter	Description
ap-lacp-striping-ip	Shows references to AP LACP LMS map information.

Example

The following is an example for execution of the `show references ap-lacp-striping-ip` command:

```
(host) [mynode] #show references ap-lacp-striping-ip
```

Related Commands

Command	Description
ap-lacp-striping-ip	Configures the AP LACP LMS map information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ap-name

```
show references
  ap-name <profile-name>
  [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP-group profile.

Parameter	Description
ap-name <profile-name>	Shows references to an AP name profile.

Example

The following is an example for execution of the `show references ap-name` command:

```
(host) [mynode] #show references ap-name ap228
```

Related Commands

Command	Description
ap-name	Configures a specific AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references aruba-central

```
show references
  aruba-central
  [page <page>] [start <start>]
```

Description

This command shows the number of references to Aruba-Central.

Parameter	Description
aruba-central	Shows references to Aruba-Central.

Example

The following is an example for execution of the `show references aruba-central` command:

```
(host) [mynode] #show references aruba-central
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ble

```
show references ble
  service-profile <profile-name>
```

Description

This command displays references to a ble profile.

Parameter	Description
<code>service-profile <profile name></code>	Specify ble profile name.
<code>page <page></code>	Include this optional parameter to limit output of this command to the specified number of items.
<code>start <start></code>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode] #show references ble service-profile wli-test

References to Ble Service Profile "wli-test"
-----
Referrer  Count
-----  ----
Total References:0
```

Related Commands

Command	Description
ble service profile	configures Bluetooth Low Energy (BLE) service profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references bw-contract

```
show references
  bw-contract <name> [revert_cmd]
  [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Parameter	Description
<code>bw-contract <name></code>	Shows references to bandwidth contract. Specify the bandwidth contract name.
<code>[revert_cmd]</code>	List of no commands to change the value.

Example

The following is an example for execution of the `show references bw-contract` command:

```
(host) [mynode] #show references bw-contract bwcontract1
```

Related Commands

Command	Description
aaa bandwidth-contract	This command configures a bandwidth contract.
cp-bandwidth-contract	This command configures a bandwidth contract traffic rate, which can then be associated with a whitelist/allowlist session ACL.
firewall cp-bandwidth-contract	This command configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of whitelist have been replaced with allowlist .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references control-plane-security

```
show references
  control-plane-security
  [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Parameter	Description
control-plane-security	Shows references to the Control Plane Security Profile.

Example

The following is an example for execution of the `show references control-plane-security` command:

```
(host) [mynode] #show references control-plane-security
```

Related Commands

Command	Description
control-plane-security	Configures the control plane security profile by identifying APs to receive security certificates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references dump-collection-profile

```
show references dump-collection-profile {default | <profile-name>}  
[page <number>][start <number>]
```

Description

This command shows references to a dump collection profile.

Parameter	Description
{default <profile-name>}	Specify the profile for collecting core dump when an AP process crashes.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following is an example of the command that shows references to a dump collection profile,

```
(host)[mynode] #show references dump-collection-profile default  
  
References to Dump collection profile "default"  
-----  
Referrer                                     Count  
-----  
ap system-profile "default" dump-collection-profile 1  
ap system-profile "NoAuthApSystem" dump-collection-profile 1  
Total References:2
```

Related Commands

Related Command	Description
ap system-profile	This command configures the AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references est profile

```
show references
  est profile {default | <profile-name>}
  [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Parameter	Description
est profile <profile-name>	Show references to an EST Profile.

Example

The following is an example for execution of the `show references est profile` command:

```
(host) [mynode] #show references est profile default
```

Related Commands

Related Command	Description
est	This command configures an EST profile on the controller. This configuration is then pushed to the AP on successful enrollment.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references file syncing profile

```
show references
  file syncing profile
  [page <page>] [start <start>]
```

Description

This command shows references to the file syncing profile.

Parameter	Description
file syncing profile	Shows references to the file syncing profile.

Example

The following is an example for execution of the `show references file syncing profile` command:

```
(host) [mynode] #show references file syncing profile
```

Related Commands

Command	Description
file syncing profile	Allows the user to configure the file syncing profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references gps

```
show references gps
  service-profile <profile-name>
```

Description

This command displays references to a gps profile.

Parameter	Description
service-profile <profile name>	Specify gps profile name.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode] #show references gps service-profile default

References to GPS Service Profile "default"
-----
Referrer                                     Count
-----
ap-group "$(touch /flash/config/proof1)" gps-service-profile 1
ap-group "default" gps-service-profile 1
ap-group "NoAuthApGroup" gps-service-profile 1
Total References:3
```

Related Commands

Command	Description
gps	configures GPS profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references guest-access-email

```
show references
  guest-access-email
  [page <page>] [start <start>]
```

Description

This command shows references to the global guest access email profile.

Parameter	Description
guest-access-email	Shows references to the guest-access email profile.
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references guest-access-email

References to Guest-access Email Profile
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Command	Description
guest-access-email	Configures the SMTP server which is used to send guest email.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ha

```
show references
  ha group-profile <profile-name>
  [page <page>] [start <start>]
```

Description

This command displays HA group profile references.

Parameter	Description
group-profile <profile-name>	Name of the HA group profile for which you want to show references.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <page>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for a specific HA group profile.

```
(host)[mynode](config) #show references ha group-profile newgroup
References to HA group information "newgroup"
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Command	Description
ha	Creates a new high availability group, or define settings for an existing group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ids

```
show references ids
  ap-classification-rule <rule-name>
  ap-rule-matching
  dos-profile {default | <profile-name>}
  general-profile {default | <profile-name>}
  impersonation-profile {default | <profile-name>}
  management-profile
  profile {default | <profile-name>}
  rap-wml-server-profile <server-name>
  rap-wml-table-profile <table-name>
  rate-thresholds-profile {default | <profile-name>}
  signature-matching-profile {default | <profile-name>}
  signature-profile <profile-name>
  unauthorized-device-profile {default | <profile-name>}
  wms-general-profile
  wms-local-system-profile
```

Description

This command displays IDS profile references.

Parameter	Description	Default
ap-classification-rule <rule-name>	Shows references to an IDS AP classification rule profile.	
ap-rule-matching	Shows references to the IDS Active AP Rules Profile.	
dos-profile <profile-name>	Shows references to an IDS Denial of Service (DoS) profile.	default
general-profile <profile-name>	Shows references to an IDS general profile.	default
impersonation-profile <profile-name>	Shows references to an IDS impersonation profile.	default
management-profile	Shows references to the IDS WMS management profile.	
profile <profile-name>	Shows references to an IDS profile.	default

Parameter	Description	Default
rap-wml-server-profile <server-name>	Shows references to an IDS remote AP WML server profile.	
rap-wml-table-profile <table-name>	Shows references to an IDS remote AP WML table profile	
rate-thresholds-profile <profile-name>	Shows references to an IDS rate thresholds profile.	default
signature-matching-profile <profile-name>	Shows references to an IDS signature matching profile.	default
signature-profile <profile-name>	Shows references to an IDS signature profile.	default
unauthorized-device-profile <profile-name>	Shows references to an unauthorized device profile.	default
wms-general-profile	Shows references to the IDS WMS general profile.	
wms-local-system-profile	Shows references to the IDS WMS local system profile.	

Example

Execute the following command to display a list of references for the default IDS profile.

```
(host) [mynode] #show references ids profile default
References to IDS Profile "default"
-----
Referrer                                Count
-----
ap-group "default" ids-profile          1
ap-group "NoAuthApGroup" ids-profile    1
Total References:2
```

Related Commands

Command	Description
<u>ids ap-classification-rule</u>	Configures the IDS AP classification rule profile.
<u>ids ap-rule-matching</u>	Configures the IDS active AP rules profile by enabling an AP classification rule.
<u>ids dos-profile</u>	Configures traffic anomalies for denial of service (DoS) attacks.
<u>ids general-profile</u>	Configures an IDS general profile.
<u>ids impersonation-profile</u>	Configures anomalies for impersonation attacks.
<u>ids management-profile</u>	Configures the IDS WMS management profile.
<u>ids profile</u>	Defines a set of IDS profiles.
<u>ids rate-thresholds-profile</u>	Configures an IDS rate thresholds profile.
<u>ids signature-matching-profile</u>	Configures an IDS signature matching profile.
<u>ids signature-profile</u>	Configures signatures for wireless intrusion detection.
<u>ids unauthorized-device-profile</u>	Configures detection of unauthorized devices, as well as rogue AP detection and containment.
<u>ids wms-general-profile</u>	configures the IDS WLAN management system (WMS) general profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ifmap cppm

```
show references
  ifmap cppm
  [page <page>] [start <start>]
```

Description

This command displays the ClearPass Policy Manager IF-MAP references.

Parameter	Description
ifmap cppm	Shows references to the ClearPass Policy Manager IF-MAP profile.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the ClearPass Policy Manager IF-MAP profile.

```
(host) [mynode] #show references ifmap cppm
References to CPPM IF-MAP Profile
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Command	Description
ifmap	Sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references ip-flow-export-profile

```
show references
  ip-flow-export-profile
  [page <page>] [start <start>]
```

Description

This command shows references to the IP flow collector Profile.

Parameter	Description
ip-flow-export-profile	Shows references to the IP flow collector profile.
page <page>	Include this optional parameter to limit output of this command to the specified number of items.
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the IP flow export profile:

```
(host) [mynode] #show references ip-flow-export-profile
```

Related Commands

Command	Description
ip-flow-export-profile	Configures the IP flow collector profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references lc-cluster

```
show references lc-cluster group-profile <profile-name> {page<page> start<start>}
```

Description

Displays controller Cluster Profile references.

Parameter	Description
group-profile <profile-anme>	Name of the lc-cluster group profile for which you want to show references.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

```
(host) [MDC] #show references lc-cluster group-profile wli-dev-v4  
  
References to Classic Controller Cluster Profile "wli-dev-v4"  
-----  
Referrer   Count  
-----  
Total References:0
```

Related Commands

Command	Description
lc-cluster group-profile	This command is used to configure the cluster group profile in the Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Managed device.

show references lcd-menu

```
show references lcd-menu {page<number> start<number>}
```

Description

This command shows references to lcd-menu.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output. This command can be executed only on **/md subtree**. This command is not supported on Mobility Controller - Virtual Appliance platform.

Related Commands

Related Command	Description
lcd-menu	This command allows you to enable or disable the LCD menu either completely or for specific operations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Managed device.

show references license-pool-profile

```
show references
  license-pool-profile
  [page <page>] [start <start>]
```

Description

This command displays references to a License pool profile.

Parameter	Description
<code>license-pool-profile</code>	Shows references to the license-pool profile.
<code>page <page></code>	Include this parameter to limit output of this command to the specified number of items.
<code>start <start></code>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the license-pool profile.

```
(host)[node] #show references license-pool-profile
```

Related Commands

Related Command	Description
license-pool-profile	Creates a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references license-pool-profile-root

```
show references
  license-pool-profile-root
  [page <page>] [start <start>]
```

Description

This command displays references to a License root (/) pool profile.

Parameter	Description
license-pool-profile-root	Shows references to the license root (/) pool profile.
page <page>	Include this parameter to limit output of this command to the specified number of items.
start <start>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the license-pool profile.

```
(host)[node] #show references license-pool-profile-root

References to License root(/) pool profile
-----
Referrer  Count
-----  ----
Total References:0
```

Related Commands

Related Command	Description
license-pool-profile	Creates a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references mgmt-server profile

```
show references mgmt-server profile <profile_name>
```

Description

Shows the management server configuration profiles.

Parameter	Description
mgmt-server profile	Specifies the management profile name.
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode] #show references mgmt-server profile default
References to Mgmt Config profile "default"
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Related Command	Description
mgmt-server	This command configures the management server profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show references openflow-controller

```
show references openflow-controller {page<number> start<number>}
```

Description

This command shows references to openflow controller.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command show references to openflow controller,

```
(host)[mm] #show references openflow-controller
References to Openflow-controller
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Related Command	Description
openflow-controller	This command configures OpenFlow controller on the Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references openflow-profile

```
show references openflow-profile {page<number> start<number>}
```

Description

This command shows references to openflow-profile.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command show references to openflow-profile,

```
(host)[mm] #show references openflow-profile
References to Openflow-profile
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Related Command	Description
openflow-profile	This command configures openflow profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references pan

```
show references pan {active-profile [page<number> start<number>]} | {profile <default|profile-name> [page<number> start<number>]}
```

Description

This command shows references to Palo Alto Networks configuration.

Parameter	Description
active-profile	Shows references to the Palo Alto Networks Active Profile.
profile <default profile-name>	Shows references to the Palo Alto Networks Servers Profile.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command show references to Palo Alto Networks configuration,

```
(host)[mm] #show references pan active-profile
References to Palo Alto Networks Active Profile
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Related Command	Description
pan-active-profile	This command makes a Palo Alto Network profile active from a set of profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references pan-options

```
show references pan-options [page<number> start<number>]
```

Description

This command shows references to configure Palo Alto Networks options.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output. This command can be executed only on **/md subtree**.

Example

```
(host) [MDC] ##show references pan-options
References to Configure Palo Alto Networks options
-----
Referrer  Count
-----  -----
Total References:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Managed Device.

show references papi-security

```
show references papi-security [page <number>] [start <number>]
```

Description

Show references to a PAPI security profile.

Parameter	Description
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host) [node]#show references papi-security

References to PAPI Security Profile
-----
Referrer  Count
-----  ----
Total References:0
```

Related Commands

Related Command	Description
papi-security	The papi-security command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show references rf

```
show references rf
  am-scan-profile <profile-name>
  arm-profile <profile-name>
  arm-rf-domain-profile <profile-name>
  dot11-60GHz-radio-profile <profile-name>
  dot11-6GHz-radio-profile <profile-name>
  dot11a-radio-profile <profile-name>
  dot11a-secondary-radio-profile
  dot11g-radio-profile <profile-name>
  event-thresholds-profile <profile-name>
  ht-radio-profile <profile-name>
  optimization-profile <profile-name>
  spectrum-profile <profile-name>
```

Description

Show RF profile references.

Parameter	Description
am-scan-profile	Show references to an AM Scanning profile
arm-profile	Show references to an Adaptive Radio Management (ARM) profile.
arm-rf-domain-profile	Show references to the ARM RF domain profile.
dot11-60GHz-radio-profile	Show references to a 60 GHz radio profile
dot11-6GHz-radio-profile	Show references to a 6 GHz radio profile.
dot11a-radio-profile	Show references to a 802.11a radio profile.
dot11a-secondary-radio-profile	Show references to a secondary 802.11a radio profile.
dot11g-radio-profile	Show references to a 802.11g radio profile.
event-thresholds-prof	Show references to an RF Event Thresholds profile.
ht-radio-profile	Show references to a High-throughput radio profile.
optimization-profile	Show references to an RF Optimization profile.
spectrum-profile	Show references to a Spectrum profile.

Example

```
(host)[mm] #show references rf spectrum-profile default-a

References to Spectrum profile "default-a"
-----
Referrer                                     Count
-----
rf dot11a-radio-profile "default" spectrum-profile      1
rf dot11a-radio-profile "rp-maintain-a" spectrum-profile 1
rf dot11a-radio-profile "rp-monitor-a" spectrum-profile 1
rf dot11a-radio-profile "rp-scan-a" spectrum-profile     1
Total References:4
```

Related Commands

Related Command	Description
rf arm-profile	This command configures the Adaptive Radio Management (ARM) profile.

Command History

Release Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references scheduler-profile

```
show references scheduler-profile {default | <map-name> } [page<number>]
start<number>]
```

Description

This command shows references to a scheduler profile.

Parameter	Description
default <map-name>	Shows references to the default profile or to a specific profile.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command shows references to a scheduler profile,

```
(host)[mm] #show references scheduler-profile default
References to scheduler profile "default"
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Related Command	Description
scheduler-profile	Define a schedule profile that associates priorities to four uplink queues.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references sdwan-profile

```
show references sdwan-profile [page<number> start<number>]
```

Description

This command shows references of the SD-WAN profile.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command shows references of the SD-WAN profile,

```
(host)[mm] #show references sdwan-profile
References to sdwan-profile
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Command	Description
sdwan-profile	This command enables or disables an SD-WAN profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references sso idp-profile

```
show references sso idp-profile <sso_prof_name> [page<number> start<number>]
```

Description

This command shows references to an SSO profile.

Parameter	Description
<code>idp-profile <sso_prof_name></code>	Name of the SSO profile.
<code>page <number></code>	Include this parameter to limit output of this command to the specified number of items.
<code>start <number></code>	Include this parameter to start displaying the output of this command at the specified index number.

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Related Commands

Command	Description
sso-idp profile	This command configures an SSO Identity Provider profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references time-range-profile

```
show references time-range-profile <profile-name> [page<number> start<number>]
```

Description

This command shows references to a time range profile.

Parameter	Description
<profile-name>	Name of the profile.
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Command	Description
time-range-profile	This command configures a time-range-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references traceoptions

```
show references traceoptions [page<number> start<number>]
```

Description

This command shows references to traceoptions.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Command	Description
traceoptions	This command configures the traceoptions to monitor and log traffic flows.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor and Managed Device.

show references ucc

```
show references ucc
  custom-sip
  facetime
  h323
  ich
  jabber
  noe
  rtpa-config
  sccp
  session-idle-timeout
  sip
  skype4b
  teams
  vocera
  webrtc
  wificalling
    page <page>
    start <start>
```

Description

This command displays the UCC ALG references to a profile.

Parameter	Description
custom-sip	Show references to the custom-sip ALG configuration.
facetime	Show references to the Apple FaceTime ALG configuration.
h323	Show references to the H.323 ALG configuration.
ich	Show references to the Intelligent Call Handling configuration.
jabber	Show references to the Cisco Jabber ALG configuration.
noe	Show references to the Alcatel-Lucent New Office Environment (NOE) ALG configuration.
rtpa-config	Show references to the Real-Time Analysis configuration.
sccp	Show references to the Cisco SCCP ALG configuration.
session-idle-timeout	Show references to the UCC Session Idle Timeout configuration.
sip	Show references to the SIP ALG configuration.
skype4b	Show references to the Microsoft Skype for Business ALG configuration.

Parameter	Description
teams	Show references to the Microsoft Teams ALG configuration.
vocera	Show references to the Vocera ALG configuration.
webrtc	Show references to the WebRTC ALG configuration
wificalling	Show references to the Wi-Fi Calling configuration.
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references u skype4b

References to Skype4B ALG Configuration
-----
Referrer  Count
-----  -----
Total References:0
```

Related Commands

Related Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show references upgrade-profile

```
show references upgrade-profile {page<page> start<start>}
```

Description

Displays the upgrade profile references.

Parameter	Description
<code>upgrade-profile</code>	Shows references to the upgrade profile.
<code>page <number></code>	Include this parameter to limit output of this command to the specified number of items.
<code>start <number></code>	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to display a list of references for the upgrade profile.

```
(host)[mynode]#show references upgrade-profile
References to Upgrade Profile
-----
Referrer  Count
-----  ----
Total References:0
```

Related Commands

Related Command	Description
upgrade-profile	This command is used to configure the upgrade profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor

show references user-role

```
show references user-role <role_name>
```

Description

Show access rights for user role.

Parameter	Description
<role_name>	The role name assigned to a user.

Example

```
(host)[mynode] #show references user-role guest

References to User Role "guest"
-----
aaa profile "airwave-office-ssid" mac-default-role
aaa profile "amigopod-guest" mac-default-role
aaa profile "corp1344-voip" mac-default-role
aaa profile "default" mac-default-role
aaa profile "default-airwave-office" mac-default-role
aaa profile "default-corp1344" mac-default-role
aaa profile "default-corp1344-no-okc" mac-default-role
aaa profile "default-corp1344-okc" mac-default-role
aaa profile "default-dot1x" mac-default-role
aaa profile "default-dot1x-psk" mac-default-role
aaa profile "default-dot1x-psk" dot1x-default-role
aaa profile "default-India" mac-default-role
aaa profile "default-india-hotel" mac-default-role
```

Related Commands

Related Command	Description
user-role	This command configures a user role.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references websocket clearpass

```
show references websocket clearpass [page<number> start<number>]
```

Description

This command shows references to the ClearPass WebSocket profile.

Parameter	Description
page <number>	Include this parameter to limit output of this command to the specified number of items.
start <number>	Include this parameter to start displaying the output of this command at the specified index number.

Example

The following command shows references to the valid equipment OUI profile,

```
(host)[mm] #show references websocket clearpass
References to ClearPass WebSocket Profile
-----
Referrer  Count
-----  -----
Total References:0
```

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Related Commands

Related Command	Description
websocket clearpass	This command configures the ClearPass WebSocket profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Managed Device and Mobility Conductor.

show references web-server

```
show references web-server profile [page <number>] [start <number>]
```

Description

Show the Web server configuration references.

Parameter	Description
page <number>	Include this optional parameter to limit output of this command to the specified number of items.
start <number>	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references web-server profile  
  
References to Web Server Configuration  
-----  
Referrer  Count  
-----  ----  
Total References:0
```

Related Commands

Related Command	Description
web-server profile	This command configures the Mobility Conductor's web server.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show references wlan

```
show references wlan
  6ghz-rrm-ie-profile
  anyspot-profile
  bcn-rpt-req-profile
  client-wlan-profile
  dot11k-profile <profile-name>
  dot11r-profile <profile-name>
  edca-parameters-profile <profile-name>
  he-ssid-profile
  hotspot
    advertisement-profile
    anqp-3gpp-nwk-profile <profile-name>
    anqp-domain-name-profile <profile-name>
    anqp-ip-addr-avail-profile <profile-name>
    anqp-nai-realm-profile <profile-name>
    anqp-nwk-auth-profile <profile-name>
    anqp-roam-cons-profile <profile-name>
    anqp-venue-name-profile <profile-name>
    h2qp-conn-capability-profile <profile-name>
    h2qp-op-cl-profile <profile-name>
    h2qp-operator-friendly-name-profile <profile-name>
    h2qp-wan-metrics-profile <profile-name>
    hs2-profile <profile-name>
  ht-ssid-profile
  mu-edca-parameters-profile
  rrm-ie-profile
  sae-profile
  ssid-profile <profile-name>
  traffic-management-pr <profile-name>
  tsm-req-profile
  virtual-ap <profile-name>
  wmm-traffic-management
```

Description

Show information about the different configuration profiles that reference a specific WLAN profile.

Parameter	Description
6ghz-rrm-ie-profile	Shows references to an RRM IE profile for 6 GHz.
anyspot-profile	Shows references to an Anyspot profile.
bcn-rpt-req-profile	Shows references to a Beacon Report Request profile.

Parameter	Description
client-wlan-profile	Shows references for the Client WLAN profile.
dot11k-profile <profile-name>	Shows references to a 802.11k profile.
dot11r-profile <profile-name>	Shows references to a 802.11r profile.
edca-parameters-profile <profile-name>	Shows references to an EDCA parameters profile.
he-ssid-profile	Shows references to a high-efficiency SSID profile.
hotspot	Shows references to one of the following hotspot profile types: <ul style="list-style-type: none"> ■ advertisement-profile ■ anqp-3gpp-nwk-profile ■ anqp-domain-name-profile ■ anqp-ip-addr-avail-profile ■ anqp-nai-realm-profile ■ anqp-nwk-auth-profile ■ anqp-roam-cons-profile ■ anqp-venue-name-profile ■ h2qp-conn-capability-profile ■ h2qp-op-cl-profile ■ h2qp-operator-friendly-name-profile ■ h2qp-wan-metrics-profile ■ hs2-profile
ht-ssid-profile <profile-name>	Shows references to a high-throughput SSID profile.
mu-edca-parameters-profile	Shows references to an MU EDCA parameters profile.
rrm-ie-profile	Shows references to an RRM IE profile.
sae-profile	Shows references to the WPA3 SAE configuration.
ssid-profile <profile-name>	Shows references to an SSID management profile.
traffic-management-profile <profile-name>	Shows references to a traffic management profile.
virtual-ap <profile-name>	Shows references to a virtual AP profile.
tsm-req-profile	Show references to a TSM Report Request profile.
wmm-traffic-management	Shows references to a WMM Traffic management profile.

Example

The following example shows that two different WLAN hotspot 2.0 profiles reference the **default** WLAN hotspot advertisement profile.

```
(host) [mynode] #show references wlan hotspot advertisement-profile default

References to Advertisement Profile "default"
-----
Referrer                                     Count
-----
wlan hotspot hs2-profile "deploytest" advertisement-profile 1
wlan hotspot hs2-profile "default" advertisement-profile    1

Total References:2
```

Related Commands

Related Command	Description
wlan ssid-profile	This command configures an SSID profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show references zigbee

```
show references zigbee
  service-profile <profile-name>
  socket-device-profile <profile-name>
  socket-inbound-profile <profile-name>
  socket-outbound-profile <profile-name>
```

Description

Show info socket-inbound-profile rmatoin about specific zigbee profile.

Parameter	Description
<code>service-profile <profile-name></code>	Displays references to specified ZigBee service profile.
<code>socket-device-profile <profile-name></code>	Displays references to specified Zigbee socket device profile.
<code>socket-inbound-profile <profile-name></code>	Displays references to specified Zigbee socket inbound profile.
<code>socket-outbound-profile <profile-name></code>	Displays references to specified Zigbee socket outbound profile.

Example

```
(host) [mynode] #show references zigbee service-profile
```

Related Commands

Related Command	Description
zigbee service-profile	This command configures ZigBee service profile.
zigbee socket-device-profile	This command configures Zigbee socket device profile.
zigbee socket-inbound-profile	This command configures Zigbee socket inbound profile.
zigbee socket-outbound-profile	This command configures Zigbee socket outbound profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf

```
show rf
  am-scan-profile
  arm-profile
  arm-rf-domain-profile
  dot11-60GHz-radio-profile
  dot11-6GHz-radio-profile
  dot11a-radio-profile
  dot11a-secondary-radio-profile
  dot11g-radio-profile
  event-thresholds-profile
  ht-radio-profile
  optimization-profile
  spectrum-profile
```

Description

This command shows the rf configuration settings. Click parameter links to view the corresponding show commands.

Parameter	Description
am-scan-profile	Shows an AM Scanning profile.
arm-profile	Shows an Adaptive Radio Management (ARM) profile.
arm-rf-domain-profile	Shows the ARM RF domain.
dot11-60GHz-radio-profile	Shows a 60 GHz radio profile.
dot11-6GHz-radio-profile	Shows a 6 GHz radio profile.
dot11a-radio-profile	Shows an 802.11 a radio profile.
dot11a-secondary-radio-profile	Shows an 802.11 a secondary radio profile.
dot11g-radio-profile	Shows an 802.11 g radio profile.
event-thresholds-profile	Shows an RF Event Thresholds Profile.
ht-radio-profile	Shows a High-throughput radio profile.
optimization-profile	Shows an RF Optimization Profile.
spectrum-profile	Shows a Spectrum profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf am-scan-profile

```
show rf am-scan-profile [<profile-name>]
```

Description

Display the AM scanning profile list. Optionally display parameter and values of a specified Air Monitor profile.

Parameter	Description
<profile-name>	Name of this instance of the profile.

Enter the basic show command to view a list of profiles, the number of profiles and the profile status. For example:

```
(host) [mynode]#show rf am-scan-profile

AM Scanning profile List
-----
Name       References  Profile Status
-----
default    9
north      0

Total:2
```

Example

In the example above, there are two profile names; default and north. The Reference column indicates the number of references to this profile name. The Profile Status column is blank unless the profile is predefined.

Optionally, you can enter a profile name to view the parameters for that profile. For example:

```
(host) [mynode]#show rf am-scan-profile default

AM Scanning profile "default"
-----
Parameter                               Value
-----
Scan Mode                                all-reg-domain
Dwell time: Active channels                500
Dwell time: Regulatory Domain channels    250
Dwell time: non-Regulatory Domain channels 200
Dwell time: Rare channels                  100
```

The explanation of the display output is described in the table below.

Parameter	Description
Scan-mode	The scanning mode for the radio
all-reg-domain	Scan channels in all regulatory domain
rare	Scan all channels (all regulatory domains and rare channels)
reg-domain	Scan channels in the APs regulatory domain
Dwell time: Active channels	Dwell time (in ms) for channels where there is wireless activity
Dwell time: Regulatory Domain channels	Dwell time (in ms) for AP's Regulatory domain channels
Dwell time: non-Regulatory Domain channels	Dwell time (in ms) for channels not in the APs regulatory domain
Dwell time: Rare channels	Dwell time (in ms) for rare channels

Related Commands

Related Command	Description
rf am-scan-profile	This command configures an Air Monitor (AM) scanning profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf arm-rf-domain-profile

```
show rf arm-rf-domain profile
```

Description

This profile contains a non-editable key defined by Mobility Conductor, and used to sign over-the air (OTA) ARM updates exchanged between APs.

No parameters

Example

The output of this command displays the OTA key defined by Mobility Conductor.

```
(host)[mynode] #show rf arm-rf-domain-profile

ARM RF domain
-----
Parameter          Value
-----
ARM RF domain key  27f71ad66f28c374a8904b4a82177e2c
```

Related Commands

Related Command	Description
rf arm-rf-domain-profile	This profile holds a non-editable key defined by Mobility Conductor, and used to sign over-the air (OTA) ARM updates exchanged between APs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf arm-profile

```
show rf arm-profile [<profile>]
```

Description

Show an ARM profile.

Parameter	Description
<profile>	Name of an ARM profile.

Issue this command without the <profile> parameter to display the entire ARM profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured ARM profiles. The **References** column lists the number of other profiles with references to the ARM profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[node] # show rf arm-profile
Adaptive Radio Management (ARM) profile List
-----
Name                References  Profile Status
----                -
airwave             2
default             4
default-AP85        2
no-scanning         1
Wireless-rf-profile                1

Total:5.
This example displays the configuration settings for the profile Wireless_rf_
profile.
(host)[node] #show rf arm-profile default
Adaptive Radio Management (ARM) profile "Wireless_rf_profile"
-----
-----
Parameter
  Value
-----
-----
Assignment
  single-band
```

Allowed bands for 40MHz channels

a-only

80MHz support

Enabled

160MHz-support

None

Client Aware

Enabled

Max Tx EIRP

127 dBm

Min Tx EIRP

9 dBm

Rogue AP Aware

Disabled

Scan Interval

10 sec

Aggressive scanning

true

Active Scan

Disabled

ARM Over the Air Updates

Enabled

Scanning

Enabled

Multi Band Scan

Enabled

VoIP Aware Scan

Enabled

Power Save Aware Scan

Disabled

Video Aware Scan

Enabled

Ideal Coverage Index

10

Acceptable Coverage Index

4

Free Channel Index

25

Interfering AP Weight

25 %

Backoff Time

240 sec

Error Rate Threshold

50 %

Error Rate Wait Time

30 sec

Channel Quality Aware Arm

Disabled

Channel Quality Threshold

70 %

Channel Quality Wait Time

120 sec

Minimum Scan Time

8

Load aware Scan Threshold

1250000 Bps

```
Mode Aware Arm
  Disabled
Scan Mode
  all-reg-domain
Client Match
  Enabled
Client Match report interval (sec)
  30
Allows Client Match to Automatically Clear Unsteerable Clients after Ageout
  Enabled
Client Match Unsteerable Client Ageout Interval
  2 Days 0 Hours
Client Match Band Steering G Max Signal (-dBm)
  45
Client Match Band Steering A Min Signal (-dBm)
  75
Client Match Sticky Client Check Interval (sec)
  3
Client Match Sticky Client Check SNR (dB)
  25
Client Match SNR Delta Bound(dB)
  10
Client Match Sticky Min Signal
  70
Client Match Steering Timeout (sec)
  10
Client Match Load Balancing Threshold (%)
  20
Client Match IOS Steering Backoff Interval (sec)
  300
Client Match VBR Stale Entry Age (sec)
  120
Client Match Max Steering Failures
  2
Client Match Load Balancing Client Threshold
  10
Client Match Load Balancing SNR Threshold (dB)
  77
Client Match Load Balancing Signal Delta Bound (dB)
  5
Client Match 802.11v BSS Transition Management
  Enabled
Dynamic Bandwidth Switch
  Enabled
Dynamic Bandwidth Switch Wait Time (sec)
  30
Dynamic Bandwidth Switch Triggering Indicator CCA ibss Threshold (%)
  10
Dynamic Bandwidth Switch Triggering Indicator Beacon Failed Threshold
  30
Dynamic Bandwidth Switch Triggering Indicator CCA intf Threshold (%)
  30
Dynamic Bandwidth Switch Clear Time (min)
  30
```

The output of this command includes the following parameters:

Parameter	Description
Assignment	Displays the current ARM channel/power assignment mode.
Allowed bands for 40MHz channels	Shows if 40 MHz mode of operation is allowed on the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) frequency band only, on all frequency bands, or on neither frequency band.
Client Aware	Shows if the client aware feature is enabled or disabled. When enabled, the AP does not change channels when there are active clients.
Max Tx Power	The highest transmit power levels for the AP, from 0-30 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx Power setting it cannot support, this value will be reduced to the highest supported power setting.
Min Tx Power	The lowest transmit power levels for the AP, from 0-30 dBm, in 3 dBm increments. Note that power settings will not change if the Assignment option is set to disabled or maintain.
Multi Band Scan	If enabled, single-radio APs will try to scan across bands for rogue AP detection.
Rogue AP Aware	If enabled, Aruba APs may change channels to contain off-channel rogue APs with active clients. This security features allows APs to change channels even if the Client Aware setting is disabled. This setting is disabled by default, and should only be enabled in high-security environments where security requirements are allowed to consume higher levels of network resources. You may prefer to receive Rogue AP alerts via SNMP traps or syslog events.
Scan Interval	If Scanning is enabled, the Scan Interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired.
Aggressive Scanning	When the aggressive scanning feature is enabled, an AP radio with no clients will scan channels every second.

Parameter	Description
Active Scan	If enabled, the AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. Active Scan is disabled by default, and should not be enabled except under the direct supervision of Aruba Support.
Scanning	Shows if the AP has enabled or disabled AP scanning of other channels.
VoIP Aware Scan	Shows if Aruba's VoIP Intelligent Call Handling prevents any single AP from becoming congested with voice calls. If Intelligent Call Handling is enabled, you should also enable VoIP Aware Scan in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call.
Power Save Aware Scan	When enabled, the AP will not scan if Power Save is active.
Video Aware Scan	If Video Aware Scan is enabled in the ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active video session.
Ideal Coverage Index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Acceptable Coverage Index	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Free Channel Index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel.
Backoff Time	Time, in seconds, an AP backs off after requesting a new channel or power level.
Error Rate Threshold	The percentage of errors in the channel that triggers a channel change.
Error Rate Wait Time	Time, in seconds, that the error rate has to maintain or surpass the error rate threshold before it triggers a channel change.
Channel Quality Aware Arm	Shows if ARM changes are based upon an internally calculated channel quality metric. When this feature is disabled, ARM initiates channel changes based on thresholds defined in this profile, and chooses the channel based on the calculated interference index value.

Parameter	Description
Channel Quality Threshold	Displays the channel quality percentage below which ARM initiates a channel change.
Channel Quality Wait Time	If channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.
Minimum Scan Time	Time, in seconds, that a channel must be scanned before it is considered for assignment.
Load aware Scan Threshold	The traffic throughput level an AP must reach before it stops scanning, in bytes/second. A value of 0 to disables this feature.
Mode Aware Arm	If enabled, ARM will turn APs into AMs if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
Scan Mode	<p>This parameter defines the scan mode for the AP.</p> <ul style="list-style-type: none"> ■ all-reg-domain: The AP scans channels within all regulatory domains. This is the default setting. ■ reg-domain: Limit the AP scans to just the regulatory domain for that AP.
Client Match	<p>The client match feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is enabled by default</p>
Client Match report interval (sec)	This interval defines how often an AP sends an updated client probe report to the controller. Each client probe report contains a list of MAC addresses for clients that have been active in the last two minutes, and the AP radio SNR values seen by those clients.
Client Match Unsteerable Client Ageout Interval	The client entries in an unsteerable client list remain in effect for the interval defined by this parameter before they age out.

Parameter	Description
Client Match Unsteerable Client Ageout	When client match and the client match unsteerable client ageout feature are enabled, the controller periodically sends APs that are not a desired AP match for a client in a list of unsteerable clients. These lists contain a list of MAC addresses for up to 128 clients that should not be steered to that AP.
Client Match Sticky Client Check Interval (sec)	Frequency at which the AP checks for client's received SNR values. If the SNR value drops below the threshold defined by the cm-sticky-snr parameter for three consecutive check intervals, that client may be moved to a different AP.
Client Match Sticky Client Check SNR (dB)	If the client's received signal strength indicator (RSSI) is above this signal-to-noise ratio (SNR) threshold, that client will be allowed to stay associated to its current AP. If the client's received signal strength is below this threshold, it may be moved to a different AP.
Client Match SNR threshold(dB)	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the AP radio is stronger than its current radio by the dB level defined by the cm-sticky-snr-thresh parameter, and the candidate radio also has a minimum signal level defined by the cm-sticky-min-signal parameter.
Client Match Sticky Min Signal	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the candidate AP radio is at or higher than the minimum signal level defined by this parameter <i>and</i> the candidate radio has a higher signal strength than the radio to which the client is currently associated. (The required improvement in signal strength can be defined using the cm-sticky-snr-delta command.)
Client Match Restriction timeout (sec)	When a client is steered from one AP to a more desirable AP, the steer timeout feature helps facilitate the move by defining the amount of time that any APs to which the client should NOT associate will not respond to the AP.
Client Match Load Balancing threshold (%)	When the client match feature is enabled, clients may be steered from a highly utilized channel on an AP to a channel with fewer clients. If a channel on an AP radio has this percentage fewer clients than another channel supported by the client, the client match feature may move clients from the busier channel to the channel with fewer clients.
Client Match VBR Stale Entry Age (sec)	The controller can maintains client match data for the maximum number of supported clients for that controller platform, showing the detected SNR values for up to 16 candidate APs per client. This table is periodically updated as APs send client probe reports to the controller. This parameter defines the amount of time that the controller should retain client match data from each client probe report.

Parameter	Description
Client Match Max Steer Failures	The controller keeps track of the number of times the client match feature failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If the client match feature attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger. This parameter defines the maximum allowed number of client match steering fails with the same trigger before the client is marked as unsteerable for that trigger.
Client Match Load Balancing Client Threshold	If an AP radio has fewer clients than the client match load balancing threshold defined by this parameter, the AP will not participate in load balancing.
Client Match Load Balancing SNR Threshold (dB)	Clients must detect a SNR from an underutilized AP radio at or above this threshold before the client match feature considers load balancing a client to that radio.
Dynamic Bandwidth Switch	ARM dynamic 80MHz/40MHz bandwidth switch when 80MHz assignment is enabled.
Dynamic Bandwidth Switch Wait Time (sec)	Minimum time in seconds during which dynamic bandwidth switch indicators have to be true to trigger a 80MHz to 40MHz bandwidth change.
Dynamic Bandwidth Switch Triggering Indicator CCA ibss Threshold (%)	Dynamic Bandwidth Switch wait time window starts when load aware scan rejects increases and CCA ibss is below the threshold.
Dynamic Bandwidth Switch Triggering Indicator Beacon Failed Threshold	Dynamic Bandwidth Switch beacon failed indicator is true if beacon failed num is no less than this threshold during the wait time window.
Dynamic Bandwidth Switch Triggering Indicator CCA intf Threshold (%)	Dynamic Bandwidth Switch CCA intf indicator is true if CCA intf is no less than this threshold during the wait time window.
Dynamic Bandwidth Switch Clear Time (min)	Dynamic Bandwidth Switch back to 80MHz channel after the clear time in minutes if currently there is no high volume of traffic.

Related Commands

Related Command	Description
rf arm-profile	This command configures the Adaptive Radio Management (ARM) profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf dot11-6GHz-radio-profile

```
show rf dot11-6GHz-radio-profile
  default
```

Description

This command displays an 802.11 6 GHz radio profile.

Parameter	Description
<profile>	Name of a 802.11 6 GHz profile.

Execute this command to display the 802.11 profile list including a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has configured 802.11 6 GHz radio.

```
(host)[mynode] #show rf dot11-6gHz-radio-profile default
6GHz radio profile "default"
-----
Parameter                               Value
-----
Radio enable                             Enabled
Mode                                     ap-mode
Channel                                  N/A
Transmit EIRP                            15.0 dBm
Enable CSA                               Disabled
CSA Count                                 4
Spectrum Monitoring                      Disabled
Spectrum Monitoring Profile              default-6ghz
Advertise 802.11d and 802.11h Capabilities Enabled
Beacon Period                             100 msec
```

```

Advertised regulatory max EIRP          0
ARM/WIDS Override                       OFF
Frame Bursting Mode                     Dynamic
Management Frame Throttle interval     1 sec
Management Frame Throttle Limit        30
Maximum Distance                        0 meters
Adaptive Radio Management (ARM) Profile default-6ghz
High-throughput Radio Profile          default-6ghz
AM Scanning Profile                     default
Max Channel Bandwidth                   160MHz
Min Channel Bandwidth                   80MHz
Min EIRP                                 15 dBm
Max EIRP                                 21 dBm
EIRP offset                             0 dB
Deploy changes daily at                 N/A
Association Boost                        Disabled
RTS Mode                                default
Dynamic fragmentation level             Level-0
HE duration based RTS                   1023
HE Guard Interval                       800ns 1600ns 3200ns
HE MU-OFDMA                             Enabled
HE MU-MIMO                              Enabled
HE UL MU-MIMO                           Disabled
Individual TWT                          Enabled
HE TXBF                                 Enabled
HE Supported MCS map                    11,11,11,11,11,11,11,11
Min MPDU start spacing                  0 usec
Maximum MPDU size                       11454 bytes
Max received A-MPDU size                 65535 bytes
Max transmitted A-MPDU size              65535 bytes
Basic Rates                             6 12 24
Transmit Rates                           6 9 12 18 24 36 48 54
Beacon Rate                             default
Enable Agile Multiband (MBO) for 6GHz Radio Disabled
Advertise 802.11k Capability for 6GHz Radio Disabled
Advertise AP Name for 6GHz Radio        Disabled
Advertise Location Info                  Disabled
Disable Probe Retry                      Enabled
RRM IE Settings Profile for 6GHz        default

```

Related Commands

Related Command	Description
rf dot11-6ghz-radio-profile	This command configures the radio settings for a 802.11 6 GHz radio profile in the applicable access points.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameters, Frame Bursting Mode and RTS Mode were introduced.
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show rf dot11-60GHz-radio-profile

```
show rf dot11-60GHz-radio-profile  
default
```

Description

This command displays an 802.11 60 GHz radio profile.

Parameter	Description
<profile>	Name of a 802.11 60 GHz profile.

Execute this command to display the 802.11 profile list including a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has configured 802.11.

```
(host)[mynode] #show rf dot11-60GHz-radio-profile  
802.11 60GHz radio profile List  
-----  
Name      References  Profile Status  
-----  
default   2
```

The example below shows that the controller has configured 802.11 for the profile "default".

```
(host)[mynode] #show rf dot11-60GHz-radio-profile default  
802.11 60GHz radio profile "default"  
-----  
Parameter  Value  
-----  
Channel    N/A
```

Related Commands

Related Command	Description
rf dot11-60GHz-radio-profile	This command configures AP radio settings for the 60 GHz frequency band on a 802.11 60 GHz radio profile.

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show rf dot11a-radio-profile

```
show rf dot11a-radio-profile [<profile>]
```

Description

Show an 802.11a radio profile.

Parameter	Description
<profile>	Name of an 802.11a profile.

Issue this command without the <profile> parameter to display the entire 802.11a Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured 802.11a Radio profiles. The **References** column lists the number of other profiles with references to the 802.11a Radio profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]# show rf dot11a-radio-profile
802.11a radio profile List
-----
Name           References  Profile Status
----           -
default        18
default-AP85   1
test           1
Total:3.
```

This example displays the configuration settings for the profile default.

```
(host) # show rf dot11a-radio-profile default
802.11a radio profile "default"
Parameter                               Value
-----
Radio enable                             Enabled
Mode                                     ap-mode
High throughput enable (radio)           Enabled
Very high throughput enable (radio)      Enabled
Channel                                   N/A
Transmit EIRP                             15 dBm
Non-Wi-Fi Interference Immunity          2
Supr Immunity                             0
```

```

Enable CSA                               Disabled
CSA Count                                4
Spectrum Monitoring                       Enabled
Spectrum Monitoring Profile               default-a
Advertise 802.11d and 802.11h Capabilities Disabled
Spectrum Load Balancing                  Disabled
Spectrum Load Balancing Mode              channel
Spectrum Load Balancing Update Interval (sec) 30 seconds
Spectrum Load Balancing Threshold (%)     20 percent
Spectrum Load Balancing Domain            N/A
Beacon Period                             100 msec
Beacon Regulate                           Disabled
Advertized regulatory max EIRP            0
ARM/WIDS Override                         OFF
Reduce Cell Size (Rx Sensitivity)         0 dB
Energy Detect Threshold Offset             0 dB
Management Frame Throttle interval        1 sec
Management Frame Throttle Limit           20
Maximum Distance                          0 meters
RX Sensitivity Threshold                   0 dB
RX Sensitivity Tuning Based Channel Reuse  disable
RTS Mode                                   always-enable
Set to Radar Test Mode                    disabled
Adaptive Radio Management (ARM) Profile    default
High-throughput Radio Profile              default-a
AM Scanning Profile                       default
Enable frame transmissions                 Enabled
Max Channel Bandwidth                      80MHz
Max EIRP                                   18 dBm
Min EIRP                                   12 dBm
EIRP Offset                               0 dBm
deploy-hour                                N/A

```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.
Mode	Access Point operating mode. Available options are: <ul style="list-style-type: none"> ■ am-mode: Air Monitor mode ■ ap-mode: Access Point mode ■ apm-mode: Access Point Monitor mode ■ sensor-mode: RFprotect sensor mode
High throughput enable (radio)	Shows if high-throughput (802.11n) is enabled on the radio. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.)

Parameter	Description
	A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.
Very high throughput enable (radio)	Enable or disable support for Very High Throughput (802.11ac) on the radio. This option is enabled by default.
Channel	Channel number for the AP 802.11a, 802.11n, or 802.11ac physical layer.
Transmit EIRP	Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.
Non-Wi-Fi Interference Immunity	<p>Sets a value for 802.11 Interference Immunity. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range.</p> <p>The levels for this parameter are:</p> <ul style="list-style-type: none"> ▪ Level-0: no ANI adaptation. ▪ Level-1: noise immunity only. ▪ Level-2: noise and spur immunity. This is the default setting ▪ Level-3: level 2 and weak OFDM immunity. ▪ Level-4: level 3 and FIR immunity.
Spur Immunity	<p>Displays the spur immunity value for 802.11a radio.</p> <p>NOTE: This parameter is applicable for 130 Series access points only. The controller ignores this parameter if configured for non-130 Series access points.</p>
Enable CSA	Shows if CSAs are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count	Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.
Spectrum Monitoring	If enabled, the AP operates as a hybrid AP that can simultaneously serve clients and monitor a single channel for spectrum analysis data.

Parameter	Description
Spectrum Monitoring Profile	The spectrum monitoring profile referenced by APs using this 802.11a radio profile. For details, see rf spectrum-profile on page 1254
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
Spectrum load balancing	<p>The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.</p>
Spectrum load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.
Spectrum load balancing threshold	If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.
Spectrum load balancing domain	<p>Define a spectrum load balancing domain to manually create RF neighborhoods.</p> <p>Use this option to create RF neighborhood information for networks that have disabled ARM scanning and channel assignment.</p> <ul style="list-style-type: none"> ▪ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is <i>not</i> defined, ArubaOS uses ARM to calculate RF neighborhoods. ▪ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain <i>is/also</i> defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize

Parameter	Description
	RF neighborhoods defined by ARM.
Beacon Period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.
Advertised Regulatory Max EIRP	Shows if the radio is configured to work around a known issue on Cisco 7921G telephones by capping for a radio's maximum EIRP. When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons. The supported value is 1-31 dBm.
ARM/WIDS Override	If enabled, this option disables ARM and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.
Reduce Cell Size (Rx Sensitivity)	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.
Energy Detect Threshold Offset	This parameter can modify the energy detect threshold used by the radio in making transmit decisions. The energy detect threshold is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. A value of 0 indicates the AP is using the default energy detect threshold for this radio. (This value may vary by AP model)
Frame Bursting Mode	The frame bursting mode of the AP. <ul style="list-style-type: none"> ■ Dynamic: Frame bursting is enabled only when one active client is connected to the AP, and frame bursting is disabled when there is more than one active client. ■ OFF: Frame bursting mode is always disabled. ■ ON: Frame bursting mode is always enabled.

Parameter	Description
Management Frame Throttle Interval	Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km..
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBm to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
RX Sensitivity Tuning Based Channel Reuse	Shows if the channel reuse feature's current operating mode, static, dynamic or disable. <ul style="list-style-type: none"> ▪ Static: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ▪ Dynamic: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ▪ Disable: This mode does not support the tuning of the CCA Detect Threshold.
RTS Mode	RTS mode configured to control RTS frame transmission to the clients. <ul style="list-style-type: none"> ▪ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ▪ always-disable: RTS is not used for any transmission.

Parameter	Description
	<ul style="list-style-type: none"> ▪ default: The default RTS mode configured in the wireless driver of the AP is used.
Set to Radar Test Mode	For internal use only.
Adaptive Radio Management (ARM) Profile	Name of an ARM profile associated with this 802.11a profile.
High-throughput Radio Profile	Name of a High Throughput Radio profile associated with this 802.11a profile.
AM Scanning Profile	The AM scanning profile referenced by APs using this 802.11a radio profile. For details, see rf am-scan-profile on page 1146
Max Channel Bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Conductor managed devices.
Min Channel Bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Conductor managed devices.
Max EIRP	The maximum transmission power level from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.
Min EIRP	The minimum transmission power level (in dBm) to be assigned to the AP radio(s).
EIRP Offset	This parameter is used to manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.
deploy-hour	<p>Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device.</p> <p>NOTE: If this parameter is set in both the AirMatch profile and radio profile, the setting in the radio profile will take precedence.</p>

Related Commands

Related Command	Description
rf dot11a-radio-profile	This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile for standalone controllers and the high-throughput (802.11n) radio profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameters, Frame Bursting Mode and RTS Mode were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show rf dot11a-secondary-radio-profile

```
show rf dot11a-secondary-radio-profile [<profile>]
```

Description

Shows an 802.11a secondary radio profile.

Parameter	Description
<profile>	Name of an 802.11a profile.

Issue this command without the <profile> parameter to display the 802.11a Secondary Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured 802.11a Radio profiles. The **References** column lists the number of other profiles with references to the 802.11a Radio profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] #show rf dot11a-secondary-radio-profile
802.11a secondary radio profile List
-----
Name   References  Profile Status
----  -
Total:0
```

Related Commands

Related Command	Description
rf dot11a-radio-profile	This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile for standalone controllers and the high-throughput (802.11n) radio profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameters, Frame Bursting Mode and RTS Mode were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show rf dot11g-radio-profile

```
show rf dot11g-radio-profile [<profile>]
  default
  rp-maintain-g
  rp-monitor-g
  rp-scan-g
```

Description

Show an 802.11g Radio profile.

Parameter	Description
<profile>	Name of a 802.11g profile.

Issue this command without the <profile> parameter to display the entire 802.11g profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured 802.11g profiles. The **References** column lists the number of other profiles with references to the 802.11g profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) [mynode] #show rf dot11g-radio-profile
802.11g radio profile List
-----
Name           References  Profile Status
----           -
default        2
rp-maintain-g  0
rp-monitor-g   0
rp-scan-g      0

Total:4
```

This example displays the configuration settings for the profile **default**.

```
(host) [mynode] #show rf dot11g-radio-profile default
802.11g radio profile "default"
-----
Parameter                               Value
-----
```

```

Radio enable                               Enabled
Mode                                       ap-mode
AM tx mute (radio)                        Disabled
High throughput enable (radio)            Enabled
High efficiency enable (radio)            Enabled
Very high throughput rates enable (256-QAM) Disabled
Channel                                    N/A
Transmit EIRP                             15.0 dBm
Non-Wi-Fi Interference Immunity           2
Enable CSA                                 Disabled
CSA Count                                  4
Spectrum Monitoring                        Disabled
Smart Antenna                             Disabled
Spectrum Monitoring Profile                default-g
Advertise 802.11d and 802.11h Capabilities Disabled
Spectrum Load Balancing                   Disabled
Spectrum Load Balancing Mode              channel
Spectrum Load Balancing Update Interval (sec) 30 seconds
Spectrum Load Balancing Threshold (%)      20 percent
Spectrum Load Balancing Domain            N/A
Beacon Period                             100 msec
Beacon Regulate                           Disabled
Advertised regulatory max EIRP            0
ARM/WIDS Override                         OFF
Reduce Cell Size (Rx Sensitivity)         0 dB
Energy Detect Threshold Offset            0 dB
Management Frame Throttle interval        1 sec
Management Frame Throttle Limit          30
Maximum Distance                          0 meters
RTS Mode                                   default
RX Sensitivity Threshold                  0 dB
RX Sensitivity Tuning Based Channel Reuse  disable
Protection for 802.11b Clients            Enabled
Adaptive Radio Management (ARM) Profile    default-g
High-throughput Radio Profile             default-g
AM Scanning Profile                       default
Enable frame transmissions                Enabled
Max Channel Bandwidth                     20MHz
Min Channel Bandwidth                     20MHz
Min EIRP                                   6 dBm
Max EIRP                                   12 dBm
EIRP offset                               0 dB
Deploy changes daily at                   N/A
AirMatch Mode Aware                       Disabled
Association Boost                          Disabled
IoT Coexistence                           Enabled

```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.

Parameter	Description
Mode	<p>Access Point operating mode. Available options are:</p> <ul style="list-style-type: none"> ▪ am-mode: Air Monitor mode ▪ ap-mode: Access Point mode ▪ apm-mode: Access Point Monitor mode ▪ sensor-mode: RFprotect sensor mode
High throughput enable (radio)	<p>Shows if high-throughput (802.11n) is enabled on the radio. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.)</p> <p>A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.</p>
Very High Throughput Rates Enable	<p>Enable or disable support for Very High Throughput (802.11ac) on the radio. This option is enabled by default.</p>
Channel	<p>Channel number for the AP 802.11a, 802.11n, or 802.11ac physical layer.</p>
Transmit EIRP	<p>Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.</p>
Non-Wi-Fi Interference Immunity	<p>Sets a value for 802.11 Interference Immunity. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range.</p> <p>The levels for this parameter are:</p> <ul style="list-style-type: none"> ▪ Level-0: no ANI adaptation. ▪ Level-1: noise immunity only. ▪ Level-2: noise and spur immunity. This is the default setting ▪ Level-3: level 2 and weak OFDM immunity. ▪ Level-4: level 3 and FIR immunity.
Enable CSA	<p>Shows if CSAs are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.</p>
CSA Count	<p>Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.</p>

Parameter	Description
Spectrum Monitoring	If enabled, the AP operates as a hybrid AP that can simultaneously serve clients and monitor a single channel for spectrum analysis data.
Spectrum Monitoring Profile	The spectrum monitoring profile referenced by APs using this 802.11a radio profile. For details, see rf spectrum-profile on page 1254
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
Spectrum load balancing	<p>The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests.</p> <p>If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.</p>
Spectrum load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.
Spectrum load balancing threshold	If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.
Spectrum load balancing domain	<p>Define a spectrum load balancing domain to manually create RF neighborhoods.</p> <p>Use this option to create RF neighborhood information for networks that have disabled ARM scanning and channel assignment.</p> <ul style="list-style-type: none"> ▪ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is <i>not</i> defined, ArubaOS uses ARM to calculate RF neighborhoods. ▪ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain <i>is/so</i>

Parameter	Description
	<p>defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.</p>
Beacon Period	<p>Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.</p>
Beacon Regulate	<p>If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.</p>
Advertised Regulatory Max EIRP	<p>Shows if the radio is configured to work around a known issue on Cisco 7921G telephones by capping for a radio's maximum EIRP. When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons. The supported value is -31 dBm.</p>
ARM/WIDS Override	<p>If enabled, this option disables ARM and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.</p>
Reduce Cell Size (Rx Sensitivity)	<p>The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.</p>
Energy Detect Threshold Offset	<p>This parameter can modify the energy detect threshold used by the radio in making transmit decisions. The energy detect threshold is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. A value of 0 indicates the AP is using the default energy detect threshold for this radio. (This value may vary by AP model).</p>
Management Frame Throttle Interval	<p>Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.</p>

Parameter	Description
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km..
RTS Mode	<p>RTS mode configured to control RTS frame transmission to the clients.</p> <ul style="list-style-type: none"> ▪ always-enable: RTS is used for every PPDU/ A-MPDU transmission. ▪ always-disable: RTS is not used for any transmission. ▪ default: The default RTS mode configured in the wireless driver of the AP is used.
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBm to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
RX Sensitivity Tuning Based Channel Reuse	<p>Shows if the channel reuse feature's current operating mode, static, dynamic or disable.</p> <ul style="list-style-type: none"> ▪ Static: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ▪ Dynamic: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ▪ Disable: This mode does not support the tuning of the CCA Detect Threshold.

Parameter	Description
Protection for 802.11b Clients	Shows if the profile has enabled or disabled protection for 802.11b clients.
Adaptive Radio Management (ARM) Profile	Name of an Adaptive Radio Management profile associated with this 802.11a profile.
High-throughput Radio Profile	Name of a High Throughput Radio profile associated with this 802.11a profile.
AM Scanning Profile	The AM scanning profile referenced by APs using this 802.11a radio profile. For details, see rf am-scan-profile on page 1146
Max Channel Bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Conductormanaged devices.
Min Channel Bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Conductormanaged devices.
Max EIRP	Maximum EIRP from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.
Min EIRP	The minimum transmission power level (in dBm) to be assigned to the AP radio(s).
EIRP Offset	This parameter is used to manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.
deploy-hour	The hour during which AirMatch updates are sent to APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Conductor, the AirMatch solution will be deployed according to the time zone of the managed device. NOTE: If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.
AirMatch Mode Aware	Shows the status of the AirMatch Mode Aware feature. NOTE: If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.

Related Commands

Related Command	Description
rf dot11g-radio-profile	This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Command History

Release	Modification
ArubaOS 8.11.0.0	The output parameter, RTS Mode was introduced.
ArubaOS 8.10.0.0	The <code>AirMatch Mode Aware</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show rf event-thresholds-profile

```
show rf event-thresholds-profile [<profile>]
```

Description

Show an Event Thresholds profile.

Parameter	Description
<profile>	name of an Event Thresholds profile

Issue this command without the <profile> parameter to display the entire Event Thresholds profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Event Thresholds profiles. The **References** column lists the number of other profiles with references to the Event Thresholds profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host)[mynode]# show rf event-thresholds-profile
RF Event Thresholds Profile List
-----
Name           References  Profile Status
-----
default        6
event1         2
Total: 2.
```

This example displays the configuration settings for the profile **default**.

```
(host)[mynode]# show rf event-thresholds-profile default
RF Event Thresholds Profile "default"
-----
Parameter                                           Value
-----
Detect Frame Rate Anomalies                        Disabled
Bandwidth Rate High Watermark                      0 %
Bandwidth Rate Low Watermark                       0 %
Frame Error Rate High Watermark                    0 %
Frame Error Rate Low Watermark                     0 %
Frame Fragmentation Rate High Watermark            16 %
Frame Fragmentation Rate Low Watermark              8 %
Frame Low Speed Rate High Watermark                 16 %
```

```

Frame Low Speed Rate Low Watermark      8 %
Frame Non Unicast Rate High Watermark    0 %
Frame Non Unicast Rate Low Watermark     0 %
Frame Receive Error Rate High Watermark  16 %
Frame Receive Error Rate Low Watermark   8 %
Frame Retry Rate High Watermark          16 %
Frame Retry Rate Low Watermark           8 %

```

The output of this command includes the following parameters:

Parameter	Description
Detect Frame Rate Anomalies	Shows of the profile enables or disables detection of frame rate anomalies.
Bandwidth Rate High Watermark	If bandwidth in an AP exceeds this value, it triggers a bandwidth exceeded condition . The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.
Bandwidth Rate Low Watermark	If an AP triggers a bandwidth exceeded condition, the condition persists until bandwidth drops below this value.
Frame Error Rate High Watermark	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a frame error rate exceeded condition.
Frame Error Rate Low Watermark	If an AP triggers a frame error rate exceeded condition, the condition persists until the frame error rate drops below this value.
Frame Fragmentation Rate High Watermark	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, it triggers a frame fragmentation rate exceeded condition.
Frame Fragmentation Rate Low Watermark	If an AP triggers a frame fragmentation rate exceeded condition, the condition persists until the frame fragmentation rate drops below this value.
Frame Low Speed Rate High Watermark	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, it triggers a low-speed rate exceeded condition.
Frame Low Speed Rate Low Watermark	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value.
Frame Non Unicast Rate High Watermark	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, it triggers a non-unicast rate exceeded condition. This value depends upon the applications used on the network.

Parameter	Description
Frame Non Unicast Rate Low Watermark	If an AP triggers a non-unicast rate exceeded condition, the condition persists until the non-unicast rate drops below this value.
Frame Receive Error Rate High Watermark	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a frame receive error rate exceeded condition.
Frame Receive Error Rate Low Watermark	If an AP triggers a frame receive error rate exceeded condition, the condition persists until the frame receive error rate drops below this value.
Frame Retry Rate High Watermark	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, it triggers a frame retry rate exceeded condition.
Frame Retry Rate Low Watermark	If an AP triggers a frame retry rate exceeded condition exists, the condition persists until the frame retry rate drops below this value.

Related Commands

Related Command	Description
rf event-thresholds-profile	This command configures the event thresholds profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf ht-radio-profile

```
show rf ht-radio-profile [<profile>]
  default-a
  default-g
```

Description

Show a High-throughput Radio profile.

Parameter	Description
<profile>	Name of a High-throughput Radio profile.

Issue this command without the <profile> parameter to display the entire High-throughput Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured High-throughput Radio profiles. The **References** column lists the number of other profiles with references to the High-throughput Radio profile, and the **Profile Status** column indicates whether the profile is predefined and editable, and if that predefined profile has been changed from its default settings. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] #show rf ht-radio-profile
High-throughput radio profile List
-----
Name           References  Profile Status
----           -
default-a     4           Predefined (changed)
default-g     4           Predefined (changed)
Total:2
```

This example displays the configuration settings for the predefined profile **default-a**.

```
(host) [mynode] #show rf ht-radio-profile default-a
High-throughput radio profile "default-a" (Predefined (changed))
-----
Parameter                               Value
-----
40 MHz intolerance                       Disabled
Honor 40 MHz intolerance                 Enabled
CSD override                             Disabled
VHT Bandwidth Signaling                  Disabled
```

```
VHT - Transmit Beamforming Sounding Interval 0 msec
BSS Color 0
BSS Color Switch Count 10
```

This example displays the configuration settings for the predefined profile **default-g**.

```
(host) [mynode] #show rf ht-radio-profile default-g
High-throughput radio profile "default-g" (Predefined (changed))
-----
Parameter                               Value
-----
40 MHz intolerance                       Disabled
Honor 40 MHz intolerance                 Enabled
CSD override                             Disabled
VHT Bandwidth Signaling                  Disabled
VHT - Transmit Beamforming Sounding Interval 0 msec
BSS Color 0
BSS Color Switch Count 10
```

The output of this command includes the following parameters:

Parameter	Description
40 MHz intolerance	Shows whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.
Honor 40 MHz intolerance	If this parameter is enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Diversity Spreading Workaround	When this feature is enabled, all legacy transmissions will be sent using a single antenna. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n cyclic shift diversity data. This feature is disabled by default and should be kept disabled unless necessary.
BSS Color	Displays the bss color code.
BSS Color Switch Count	Displays the number of times the BSS color switch announcements are sent before switching to a new color.

Related Commands

Related Command	Description
rf ht-radio-profile	This command configures high-throughput AP radio settings. High-throughput features use the IEEE 802.11n standard.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf optimization-profile

show rf optimization-profile [<profile>]

Description

Show an Optimization profile.

Parameter	Description
<profile>	name of an ARM profile

Issue this command without the <profile> parameter to display the entire Optimization profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Optimization profiles. The **References** column lists the number of other profiles with references to the Optimization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]# show rf optimization-profile
RF Optimization Profile List
-----
Name      References  Profile Status
----      -
default   6
profile2  1

Total:2
```

This example displays the configuration settings for the profile **profile2**.

```
(host)[mynode]#show rf optimization-profile profile2
RF Optimization Profile "profile2"
-----
Parameter                               Value
-----
Station Handoff Assist                   Disabled
Detect Association Failure                Disabled
Coverage Hole Detection                   Disabled
Hole Good RSSI Threshold                   20
Hole Good Station Ageout                   30 sec
Hole Detection Interval                   180 sec
Hole Idle Station Ageout                   90 sec
```

```

Hole Poor RSSI Threshold          10
Detect interference                Disabled
Interference Threshold            90 %
Interference Threshold Exceed Time 25 sec
Interference Baseline Time        25 sec
RSSI Falloff Wait Time            4
Low RSSI Threshold                10
RSSI Check Frequency              3 sec

```

This example displays the configuration settings for the profile **default**.

```

(host)[mynode] #show rf optimization-profile default
RF Optimization Profile "default"
-----
Parameter                Value
-----
Station Handoff Assist   Disabled
RSSI Falloff Wait Time   4 sec
Low RSSI Threshold       10
RSSI Check Frequency     3 sec

```

The output of this command includes the following parameters:

Parameter	Description
Station Handoff Assist	If enabled, this parameter allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold.
Detect Association Failure	Shows if the profile enables or disables STA association failure detection.
Coverage Hole Detection	Shows if the profile enables or disables coverage hole detection.
Hole Good RSSI Threshold	Time, in seconds, after a coverage hole is detected until a coverage hole event notification is generated. This parameter requires the RF Protect license.
Hole Good Station Ageout	Stations with signal strength above this value are considered to have good coverage. This parameter requires the RF Protect license.
Hole Detection Interval	Time, in seconds, after which a station with good coverage is aged out. This parameter requires the RF Protect license.
Hole Idle Station Ageout	Time, in seconds, after which a station in a poor coverage area is aged out. This parameter requires the RF Protect license.

Parameter	Description
Hole Poor RSSI Threshold	Stations with signal strength below this value will trigger detection of a coverage hole. This parameter requires the RF Protect license.
Detect interference	Enables or disables interference detection.
Interference Threshold	Percentage increase in the frame retry rate or frame receive error rate before interference monitoring begins on a given channel.
Interference Threshold Exceed Time	Time, in seconds, the FRR or FRER exceeds the threshold before interference is reported.
Interference Baseline Time	Time, in seconds, the air monitor should learn the state of the link between the AP and client to create frame retry rate and frame receive error rate baselines.
RSSI Falloff Wait Time	Number of times the detected client RSSI level must fall below the minimum RSSI threshold the before the AP sends a deauthorization message to the client. The maximum value is 8 times.
Low RSSI Threshold	Minimum RSSI above which deauthorization messages should never be sent.
RSSI Check Frequency	Interval, in seconds, to sample RSSI.

Related Commands

Related Command	Description
rf optimization-profile	This command configures the RF optimization profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rf spectrum-profile

```
rf spectrum-profile <profile-name>
  default-a
  default-g
```

Description

Show a spectrum profile used by the spectrum analysis feature.

Parameter	Description
<profile>	Name of a spectrum profile.

Issue this command without the <profile> parameter to display the entire spectrum profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured spectrum profiles. The **References** column lists the number of other profiles with references to the spectrum profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] #show rf spectrum-profile
Spectrum profile List
-----
Name           References  Profile Status
----           -
default-a     4           Predefined (changed)
default-g     4           Predefined (changed)
Total:2
```

This example displays the configuration settings for the profile **default-a**.

```
(host)[mynode] #show rf spectrum-profile default-a
Spectrum profile "default-a" (Predefined (changed))
-----
Parameter                                           Value
-----
IP address to forward captured FFTs to             N/A
Age Out: WIFI                                       600 sec
Age Out: Generic Interferer                         30 sec
Age Out: Microwave                                 15 sec
Age Out: Microwave (Inverter type)                 15 sec
```

```

Age Out: Video Device          60 sec
Age Out: Audio Device         10 sec
Age Out: Cordless Phone Fixed Frequency 10 sec
Age Out: Generic Fixed Frequency 10 sec
Age Out: Bluetooth            25 sec
Age Out: Xbox                  25 sec
Age Out: Cordless Network Frequency Hopper 60 sec
Age Out: Cordless Base Frequency Hopper 240 sec
Age Out: Generic Frequency Hopper 25 sec
Age Out: LTE-U Fixed Frequency 10 sec
Channel                        N/A
Filter Channel                 N/A
No WiFi FFT                    0
AP mode FFT dwell time        20
FFT Format                      1

```

The output of this command includes This example displays the configuration settings for the profile **default-g**.

```

(host)[mynode] #show rf spectrum-profile default-g
Spectrum profile "default-g" (Predefined (changed))
-----
Parameter                               Value
-----
IP address to forward captured FFTs to  N/A
Age Out: WIFI                            600 sec
Age Out: Generic Interferer              30 sec
Age Out: Microwave                       15 sec
Age Out: Microwave (Inverter type)       15 sec
Age Out: Video Device                    60 sec
Age Out: Audio Device                    10 sec
Age Out: Cordless Phone Fixed Frequency  10 sec
Age Out: Generic Fixed Frequency         10 sec
Age Out: Bluetooth                       25 sec
Age Out: Xbox                            25 sec
Age Out: Cordless Network Frequency Hopper 60 sec
Age Out: Cordless Base Frequency Hopper  240 sec
Age Out: Generic Frequency Hopper        25 sec
Age Out: LTE-U Fixed Frequency           10 sec
Channel                                  N/A
Filter Channel                           N/A
No WiFi FFT                              0
AP mode FFT dwell time                   20
FFT Format                                1

```

the following information:

Parameter	Description
Age Out: WIFI	The number of seconds for which a wifi device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 600 seconds.
Age Out: Generic Interferer	The number of seconds for which an unknown device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 30 seconds.
Age Out: Microwave	The number of seconds for which a microwave device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
Age Out: Microwave (inverter type)	The number of seconds for which an inverter microwave must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
Age Out: Video Device	The number of seconds for which a video device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 60 seconds.
Age Out: Audio Device	The number of seconds for which an audio device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
Age Out: Cordless Phone Fixed Frequency	The number of seconds for which a fixed frequency cordless phone must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
Age Out: Generic Fixed Frequency	The number of seconds for which a generic fixed frequency device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.

Parameter	Description
Age Out: Xbox	The number of seconds for which an Xbox device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
Age Out: Bluetooth	The number of seconds for which a bluetooth device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
Age Out: Cordless Network Frequency Hopper	The number of seconds for which a frequency-hopping cordless network device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 60 seconds.
Age Out: Cordless Base Frequency Hopper	The number of seconds for which a frequency-hopping cordless phone base must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 240 seconds.
Age Out: Generic Frequency Hopper	The number of seconds for which a generic frequency-hopping device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds.

Related Commands

Command	Description
rf spectrum-profile	This command configures the RF spectrum profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show rft

```
show rft
  profile
  result
  transactions
```

Description

The [rft](#) command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support.

Click parameter links to view the corresponding show commands.

Parameter	Description
profile	Shows parameters of an RFT profile.
result	Shows result of a RFT test.
transactions	Shows transaction IDs of RFT tests.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Conductor and managed device.

show rft profile

```
show rft profile
  all
  ht-link-quality
  link-quality
  raw
```

Description

Show parameters for the predefined RF test profiles.

Parameter	Description
all	Show all predefined profiles.
ht-link-quality	Show configured parameters for the predefined HT Link Quality test profile.
link-quality	Show configured parameters for the predefined Link Quality test profile.
raw	Show configured parameters for the predefined RAW test profile.

The [rft](#) command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the `show rft profile` command to view the profiles used for these RF tests.

Example

The following example is an output of the `show rft profile all` command.

```
(host) #show rft profile all
Profile RAW: Built-in profile
-----
Parameter      Value
-----
Antenna         1 and/or 2
Frame Type      Null Data
Num Packets     100
Packet Size    1500
Num Retries     3
Profile LinkQuality: Built-in profile
-----
Parameter      Value
-----
Antenna         1 and/or 2
```



```

Frame Type      Null Data
Num Packets    100 for each data-rate
Packet Size    1500
Num Retries    0
Data Rate      All rates are tried
Profile HTLinkQuality: Built-in profile
-----
Parameter      Value
-----
Antenna        1 and/or 2
Frame Type     Null Data
Num Packets    100 for each data-rate
Packet Size    1500
Num Retries    0
Data Rate      All rates are tried

```

Related Commands

Command	Description
show rft result	Shows the results of an RF test.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Conductor and managed device.

show rft result

```
show rft result
  all
  trans-id <trans-id>
```

Description

Show the results of an RF test.

Parameter	Description
all	Show the most recent test result for each test type (antenna-connectivity, link-quality or raw).
trans-id <trans-id>	Each RF test is assigned a transaction ID. Include the <code>trans-id <trans-id></code> parameters to show the test result for a specific transaction ID.

The [rft](#) command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support.

Related Commands

Command	Description
show rft transactions	Shows the most recent transaction IDs for each test type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rft transactions

```
show rft transactions
```

Description

Show transaction IDs of RF tests.

No parameters.

The [rft](#) command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the `show rft transaction` command to view the transaction IDs for the most recent test of each test type.

Example

The following example shows the transaction IDs for the latest RAW, link-quality and antenna-connectivity tests.

```
(host) [mynode] #show rft transactions
RF troubleshooting transactions
-----
Profile                Transaction ID
-----
RAW                    2001
LinkQuality            2101
AntennaConnectivity    1801
```

Related Commands

Command	Description
rft	This command is used for RF troubleshooting.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rights

```
show rights
  downloaded-user-roles
  [<name-of-a-role>]
```

Description

Displays the list of user roles in the roles table with high level details of role policies. To view role policies of a specific role specify the role name.

Parameter	Description
downloaded-user-roles	Show information about downloaded user roles.
name-of-a-role	Enter the role name to view its policy details.

Example

The output of this command shows the list of roles in the role table.

```
(host) [mynode]# show rights
RoleTable
-----
Name                ACL  Bandwidth                ACL List
      Type
----  -----
ap-role             4   Up: No Limit,Dn: No Limit  control/,ap-acl/
System
authenticated      39  Up: No Limit,Dn: No Limit  allowall/,v6-allowall/
User
default-vpn-role   37  Up: No Limit,Dn: No Limit  allowall/,v6-allowall/
User
guest               3   Up: No Limit,Dn: No Limit  http-acl/,https-acl/,dhcp-
acl/
User
guest-logon        6   Up: No Limit,Dn: No Limit  logon-
control/,captiveportal/
User
logon               1   Up: No Limit,Dn: No Limit  logon-
control/,captiveportal/
User
stateful-dot1x     5   Up: No Limit,Dn: No Limit
System
voice               38  Up: No Limit,Dn: No Limit  sip-acl/,noe-acl/,svp-
acl/,vocera-acl/
User
```

The following output displays the ACE entries of role based ACL in IPv6 Split-Tunnel forwarding mode in Remote APs:

```

(host) [mynode] #show rights split
split
-----
Priority  Source      Destination Service   Application Action
TimeRange Log
-----
- ----
1         any        any         svc-dhcp   permit
2         any        any         svc-dns    permit
3         user       fe80::/16  any-v6     permit
4         fe80::/16 user       any-v6     permit
5         any        any         any-v6     route src-nat
6         any        any         svc-v6-dhcp permit
Expired  Queue  TOS  8021P  Blacklist  Mirror  DisScan  IPv4/6  Contract
-----
         Low   ---  -----
         Low   4
         Low   4
         Low   4
         Low   4
         Low   4
         Low   6
Expired Policies (due to time constraints) = 0

```

Command History

Release	Modification
ArubaOS 8.4.0.0	The output of the command was updated to display the IPv6 ACE entries of role-based ACL in Split-Tunnel forwarding mode.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show roleinfo

```
show roleinfo
```

Description

Displays the role of the controller.

No parameters.

Example

The output of this command shows the role of the controller.

```
(host) [mynode] # show roleinfo
switchrole:master
```

Related Commands

Related Command	Description
user-role	This command configures a user role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show route-access-list

```
show route-access-list
```

Description

This command displays information about ACLs for PBR.

No parameters.

Policy-based routing is an optional feature that allows packets to be routed based on ACLs configured by the administrator. By default, when a managed device receives a packet for routing, it looks up the destination IP in the routing table and forwards the packet to the next hop router. If policy-based routing is configured, the next hop device can be chosen based on a defined access control list.

In a typical deployment scenario with multiple uplinks, the default route only uses one of the uplink next-hops for forwarding packets. If a next hop becomes unreachable, the packets will not reach their destination. If your deployment uses policy-based routing based on a next hop list, any of the uplink next hops could be used for forwarding traffic. This requires a valid ARP entry (Route-cache) in the system for all the policy-based routing next hops.

Example

The following command displays a list of configured routing access lists.

```
(host) [mynode] #show route-access-list
Router Access list table
-----
Name          Use Count  Roles
----          -
attempt1     0
pbr           0
name         1          test
Tuesday      0
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the access list.
Use Count	Number of VLANs associated with this routing access list.
Roles	User role associated with the routing access list.

Related Commands

Command	Description
ip access-list route	Configures an ACL for PBR.
ip nexthop-list	Defines a next-hop list for a routing policy.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license.	Enable or Config mode on Mobility Conductor.

show rrm dot11k

```
show rrm dot11k
  ap-channel-report
  beacon-report
  neighbor-report
  transmit-stream-report
```

Description

This command shows the 802.11k information. Click parameter links to view the corresponding show commands.

Parameter	Description
ap-channel-report	Shows AP Channel Report
beacon-report	Shows Beacon Report.
neighbor-report	Shows Neighbor Report.
transmit-stream-report	Shows Transmit Stream Measurement Report.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm dot11k admission-capacity

```
show rrm dot11k admission-capacity
```

Description

Displays the available admission capacity for voice traffic on an AP.

No parameters.

Example

The output of this command shows the available admission capacity for voice traffic on all APs.

```
(host) # show rrm dot11k admission-capacity
802.11K Available Admission Capacity for Voice
-----
Flags: B: Bandwidth based CAC, C: Call-count based CAC
      D: CAC Disabled,      E: CAC Enabled
AP Name      IP Address      Freq Band  Chan  Total  Available  Flags
-----
r-wing-94    10.16.12.247    5 GHz      40    31250  0          EC
r-wing-94    10.16.12.247    2.4 GHz    11    31250  0          EC
Num APs:2
```

Related Commands

Related Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm dot11k ap-channel-report

```
show rrm dot11k ap-channel-report
  ap-name <name-of-an-ap>
  bssid <bssid-of-an-ap>
  ip-addr <ip-address-of-an-ap>
  ip6-addr <ip-addr>
```

Description

Displays the channel information gathered by the AP. You can either specify an ap-name, bssid or ip-address of an AP to see more details.

Parameter	Description
ap-name	Enter the name of the AP.
bssid	Enter the BSSID address of the AP.
ip-addr	Enter the IP address of the AP.
ip6-addr	Enter the IPv6 address of the AP

Example

The output of this command shows the channel information for r-wing-94:94.

```
(host) [mynode]# show rrm dot11k ap-channel-report ap-name r-wing-94
802.11K AP Channel Report Details
-----
Freq Band  Channel List
-----
2.4 GHz    11,
5 GHz      36, 40, 157, 161, 165,
Num Entries:2
```

Related Commands

Related Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm dot11k beacon-report

```
show rrm dot11k beacon-report
```

Description

Displays the beacon report information sent by a client to its AP.

No parameters.

Example

The output of this command shows the beacon report for the client 00:1f:6c:7a:d4:fd.

```
(host) [mynode]# show rrm dot11k beacon-report station-mac 00:1f:6c:7a:d4:fd
802.11K Beacon Report Details
-----
Channel      BSSID                Reg Class   Antenna ID   Meas. Mode
-----
--
1            00:0b:86:6d:3e:40    0           1            Bcn Table
Num Elements:1
```

Related Commands

Related Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm dot11k neighbor-report

```
show rrm dot11k neighbor-report
  ap-name
  bssid
  ip-addr
  ip6-addr
```

Description

Displays the neighbor information for a particular AP. If the AP name or the AP's IP address is specified, the user should specify the ESSID to get the neighbor information. If the ESSID is not specified, the command will display the neighbor information for all the Virtual AP's configured on the AP.

Parameter	Description
ap-name	Identify the AP for which you want to view information.
<name-of-an-ap>	Name of an AP.
<ssid>	ESSID of the AP. If the ESSID includes spaces, you must enclose it in quotation marks.
bssid	Enter the BSSID address of the AP.
ip-addr	Enter the IP address of the AP.

Example

The output of this command shows the neighbor information for r-wing-94.

```
(host) [mynode]# show rrm dot11k neighbor-report ap-name r-wing-94
802.11K Neighbor Report Details
-----
Flags: S: Spectrum Management, Q: QoS, A: APSD, R: Radio Measurement
ESSID      BSSID      Channel  Reachability  Security
Authenticator Preference  Flags
-----
-----
r-wing-voice 00:0b:86:6d:3e:30 165      Reachable     Same          Same
 1           SR
r-wing-voice 00:0b:86:6d:3e:20 1         Reachable     Same          Same
 1           SR
r-wing-data  00:0b:86:6d:3e:40 6         Reachable     Same          Same
 1           SR
```

```
r-wing-data 00:0b:86:6d:4e:41 153 Reachable Same Same
  1 SR
Num Entries:4
```

Related Commands

Related Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm dot11k transmit-stream-report station-mac

```
show rrm dot11k transmit-stream-report station-mac <mac-addr>
```

Description

This is a diagnostic option for quick verification of received transmit stream measurement reports. Displays the contents of the transmit stream measurement reports received from a client.

Parameter	Description
mac-addr	MAC address of the client.

Related Commands

Related Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show rrm handover-trigger

```
show rrm handover-trigger station-mac <station-mac>
```

Description

This command shows handover trigger information of a station.

Syntax

Parameter	Description
<station-mac>	Mac address of the station.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show running-config

show running-config

Description

Displays the current Mobility Conductor configuration, including all pending changes that are yet to be saved. Use this command to see the complete running and pending configuration on the Mobility Conductor.

Example

The output of this command shows the running configuration on the controller.

```
(host) [mynode] #show running-config
Building Configuration...

version 8.0
hostname "host"
clock timezone PST -8
!
location "Building1.floor1"
controller config 59
crypto-local pki ServerCert default-self-signed default-self-signed
crypto-local pki PublicCert master-ssh-pub-cert master-ssh-pub-cert
ip NAT pool dynamic-srcnat 0.0.0.0 0.0.0.0
ip access-list eth name2
!
ip access-list mac name
!
ip access-list eth etherypte
deny 0x0
!
ip access-list eth validuserethacl
permit any
...
...
...
snmp-server enable trap
snmp-server trap source 0.0.0.0

process monitor log
nbapi_publish
end
```

The output of this command shows the running configuration of the management server profiles.

```
(host) [mynode] #show running-config | include mgmt
Building Configuration...
```

```
interface mgmt
mgmt-server primary-server 40.40.40.1 profile default-amp transport udp
secure
mgmt-server primary-server 2001::2 profile default-amp transport udp
secure
mgmt-server primary-server 10.1.1.11 profile default-amp transport udp
mgmt-server primary-server 20.16.11.1 profile default-ale transport udp
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to display the configured default gateway on the OOB management port for 7280 controllers.
ArubaOS 8.1.0.0	Listed primary servers with IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show sapm-bucketmap

```
show sapm-bucketmap
  essid
  verbose
```

Description

This command shows the spam-bucketmap configuration settings. Click parameter links to view the corresponding show commands.

Parameter	Description
essid	Shows bucket map for an essid.
verbose	Shows bucket history has been sent to APs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on managed devices.

show sapm-bucketmap

show sapm-bucketmap [essid <essid>]

Description

Displays the bucketmap information of the AP.

Parameter	Description
essid	Enter the ESSID of the AP.

Example

The output of this command shows bucketmap information of the AP on the Mobility Conductor.

```
(host)[mynode](config) #show sapm-bucketmap essid Zone1TestEssid
SAPM Bucketmap
-----
Item                Value
----                -
Essid               Zone1TestEssid
Generation Number   1
Read Timestamp      Fri Jul 1 19:46:33 2016 (2d:14h:55m:51s ago)
Stats               GSM_ADD events=6 GSM Lookups=0 Deletes=0
UAC 0               10.10.2.3
UAC 1               10.10.2.4
UAC 2               10.10.2.5
UAC 3               10.10.2.6
Active Map [0-31]   00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [32-63]  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [64-95]  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [96-127] 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03 00 01 02 03
Active Map [128-159] 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03 00 01 03 00
Active Map [160-191] 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01 03 00 01 03
Active Map [192-223] 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03
00 01 03 00 01 03 00 01 03 00 01 03 00 01
Active Map [224-255] 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01 00 01 00 01
Num ESSIDs:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on managed devices.

show sapm-bucketmap verbose

show sapm-bucketmap verbose

Description

Displays the bucket history has been sent to APs.

Example

The output of this command shows bucketmap information of the AP on the Mobility Conductor.

```
(host)[mynode](config) #show sapm-bucketmap verbose
Clustering is not enabled
SAPM Bucketmap History
-----
Essid  GenNum  Time  State
-----
Num ESSIDs:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on managed devices.

show sapm cluster nodestate

```
show sapm cluster nodestate [verbose]
```

Description

Displays the state of the cluster nodes.

No parameters.

Example

The output of this command shows slot details on the managed device.

```
(host)(cluster) (config)# show sapm cluster nodestate
Cluster Nodelist (Gen Num 124)
-----
Index  Node IP address Public IP address
-----
1      10.17.65.35      192.168.10.249
2      10.17.65.34      192.168.10.248
```

Related Commands

Related Command	Description
cluster-debug	This command sets are used to change the bucketmap entries and to reassign the standby AAC.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on managed devices.

show scheduler-profile

show scheduler-profile <map-name>

Description

Displays details of the scheduler profile that associates priorities to four uplink queues.

Command	Description
map-name	Displays the scheduler map name.

Examples

The following example displays the priority map of the default scheduler profile.

```
(host) [mynode] #show scheduler-profile default
scheduler profile "default"
-----
Queue      Weight  Priority-map
-----
Queue 0    0       6 7
Queue 1    0       4 5
Queue 2    0       2 3
Queue 3    0       0 1
```

Related Commands

Related Command	Description
scheduler-profile	This command defines a schedule profile that associates priorities to four uplink queues.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show scp

show scp

Description

Execute this command to view the status of the SCP server functionality of the controller or managed device.

Example

To view if the SCP server functionality on the controller or managed device is enabled or not, execute the following command:

```
(host) [mynode] #show scp
```

Related Commands

Command	Description
service	Use this command to enable the SCP server functionality on the controller or managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on controller or managed device.

show sdwan-profile

```
show sdwan-profile
```

Description

This command shows if the SD-WAN profile is enabled or disabled.

No parameters.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host)[mynode] #show sdwan-profile
sdwan-profile
-----
Parameter  Value
-----
State      Disabled
```

Related Commands

Command	Description
sdwan-profile	This command enables or disables an SD-WAN profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show serial console redirect

```
show serial console redirect
```

Description

Displays the status of Serial Console Redirect.

Examples

The following example displays the status of the serial console redirect.

```
(host) [mynode] #show serial console redirect  
Serial Console Redirect : Enabled
```

Related Commands

Related Command	Description
serial console redirect	This command configures redirect to serial console.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Conductor.

show session-acl-list

```
show session-acl-list
```

Description

Displays the list of configured session ACLs in the controller.

No parameters.

Example

The output of this command shows the session ACLs in the controller.

```
(host)[mynode] # show session-access-list
v6-icmp-acl
allow-diskservices
control
validuser
v6-https-acl
vocera-acl
icmp-acl
v6-dhcp-acl
captiveportal
v6-dns-acl
allowall
test
sip-acl
https-acl
...
...
...
v6-http-acl
dhcp-acl
http-acl
stateful-dot1x
ap-acl
svp-acl
noe-acl
stateful-kerberos
v6-logon-control
h323-acl
```

Related Commands

Related Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show slots

```
show slots
```

Description

Displays the list of slots in the managed device, including the status and card type.
No parameters.

Example

The output of this command shows slot details on the managed device.

```
(host)[mynode] # show slots
Slots
-----
Slot  Status   Card Type
----  -
1     Present   A2400
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show snmp

```
show snmp
  community
  engine-id
  inform
  servers
  trap-group
  trap-hosts
  trap-list
  trap-queue
  user-table
```

Description

This command shows the snmp configuration settings. Click parameter links to view the corresponding show commands.

Parameter	Description
community	Displays the configured snmp communities.
engine-id	Displays the configured snmp engine ID.
inform	Inform queue.
servers	Display SNMP servers from which SNMP requests received
trap-group	Displays the configured SNMP trap-groups.
trap-hosts	Displays the configured trap hosts.
trap-list	All the traps in the controller
trap-queue	Displays the Trap Queue
user-table	Displays the configured snmp users.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show snmp community

show snmp community

Description

Displays the SNMP community string details.

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp community
SNMP COMMUNITIES
-----
COMMUNITY  ACCESS      VERSION
-----
public     READ_ONLY  V1, V2c
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show snmp engine-id

show snmp engine-id

Description

This command displays the SNMP engine ID.

No parameters.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host)[mynode] #show snmp engine-id
SNMP engine ID: 000039e7000000a10a11a029 (Factory Default)
```

Related Commands

Command	Description
snmp-server	This command configures SNMP server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show snmp inform

```
show snmp inform
```

Description

Displays the length of SNMP inform queue.

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp inform stats
Inform queue size is 100
SNMP INFORM STATS
-----
HOST  PORT  INFORMS-INQUEUE  OVERFLOW  TOTAL INFORMS
-----
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show snmp servers

```
show snmp servers
```

Description

Display SNMP servers from which SNMP requests received.

Example

```
(host) # show snmp servers

SNMP SERVERS
-----
SERVER          REQUEST COUNT  TIMESTAMP
-----
15.110.188.5    630            Wed Nov 16 02:04:12 2022
15.110.188.6    630            Wed Dec 7 02:51:21 2022
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show snmp trap-group

```
show snmp trap-group
```

Description

This command displays the configured SNMP trap groups.

Example

The following example displays details of the configured SNMP trap groups:

```
(host) [mynode] # show snmp trap-group

SNMP TRAP GROUP
-----
TRAP-GROUP      ENABLED TRAPS
-----
vlanTraps       wlsxVlanLinkUp
                 wlsxVlanLinkDown
                 wlsxVlanEntryChanged
linkTraps        linkUp
                 linkDown
System          wlsxFlashSpaceOK
                 wlsxMemoryUsageOK
                 wlsxPowerSupplyOK
                 wlsxFanOK
```

The output of this command includes the following parameters:

Column	Description
Trap-Group	Shows the name of the SNMP trap group.
Enabled Traps	Shows the SNMP traps configured under the trap group.

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show snmp trap-hosts

```
show snmp trap-hosts
```

Description

Displays the configured SNMP trap hosts.

No parameters.

Example

The output of this command shows details of a SNMP trap host.

```
(host) # show snmp trap-hosts
SNMP TRAP HOSTS
-----
HOST          VERSION      SECURITY NAME  PORT   TYPE   TIMEOUT  RETRY
-----
10.16.14.1    SNMPv2c     public        162   Trap  N/A      N/A
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show snmp trap-list

show snmp trap-list

Description

Displays the list of SNMP traps.

No parameters.

Example

The output of this command shows the list of SNMP traps and the status.

```
(host) # show snmp trap-list
SNMP TRAP LIST
-----
TRAP-NAME                                CONFIGURABLE  ENABLE-STATE
-----
authenticationFailure                    Yes           Enabled
coldStart                                 Yes           Enabled
linkDown                                  Yes           Enabled
linkUp                                     Yes           Enabled
warmStart                                  Yes           Enabled
wlsxAPBssidEntryChanged                   Yes           Enabled
wlsxAPEntryChanged                        Yes           Enabled
wlsxAPImpersonation                       Yes           Enabled
wlsxAPIinterferenceCleared                Yes           Enabled
wlsxAPIinterferenceDetected               Yes           Enabled
wlsxAPRadioAttributesChanged              Yes           Enabled
wlsxAPRadioEntryChanged                   Yes           Enabled
wlsxAccessPointIsDown                     Yes           Enabled
wlsxAccessPointIsUp                       Yes           Enabled
wlsxAdhocNetwork                          Yes           Enabled
wlsxAdhocNetworkBridgeDetected            Yes           Enabled
wlsxAdhocNetworkBridgeDetectedAP         Yes           Enabled
wlsxClusterVlanProbeStatus                Yes           Disable
...
...
...
...
wlsxFanOK                                  Yes           Enabled
wlsxFanTrayInserted                       Yes           Enabled
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

Release	Modification
ArubaOS 8.11.0.0	A new SNMP trap, wlsxLicenseThresholdLimitHit was added.
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.8.0.0	A new SNMP trap, wlsxClusterVlanProbeStatus was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor/Mobility Conductor and managed devices.

show snmp trap-queue

show snmp trap-queue

Description

Displays the list of SNMP traps in queue.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp trap-queue

a)wlsxMgmtUserAuthenticationFailed
The trap indicates that a management user authentication failed.
2013-10-29 08:08:10 Management user authentication failed for user
commonuser1 with IP address 10.20.102.79 usermac 00:00:00:00:00:00 server
name CiscoACS-2 serverip 10.15.28.41
b)wlsxNUserAuthenticationFailed :
The trap indicates that a user authentication has failed.
2013-10-29 07:47:07 User Authentication failed for user commonuser1 userip
0.0.0.0 usermac 00:5f:12:00:00:00 servername CiscoACS-1 serverip 10.15.28.40
bssid 00:d2:5d:80:00:08 apname v5rapsim_000_000
c)wlsxNAuthServerReqTimeout:
The trap indicates that the authentication server req timeout
2013-10-29 07:44:58 Authentication request timed out for server CiscoACS-1
serveip 10.15.28.4 username commonuser1 userip 0.0.0.0 usermac
00:5f:12:00:00:00 bssid 00:d2:5d:80:00:08 apname v5rapsim_000_000
d)wlsxNAuthServerTimeout :
The trap indicates the server taken out of service.
2013-10-29 07:45:48 Authentication server CiscoACS-1 serverip 10.15.28.4
timed out. Time out value is 1383012948 for user commonuser1 ip 0.0.0.0 mac
00:5f:12:00:00:00 bssid 00:d2:5d:80:00:08 apname v5rapsim_000_000
e)wlsNAuthServerIsDown
The trap indicates that an authentication server is down.
2013-10-29 07:44:11 Authentication Server CiscoACS-1 with ip 10.15.28.4 is
down.
f)wlsNAuthServerUp
The trap indicates that an authentication server is up.
2013-10-29 07:45:48 Authentication server CiscoACS-1 with ip 10.15.28.4 is
up
```

Command History

Release	Modification
ArubaOS 8.11.0.0	A new SNMP trap, wlsxLicenseThresholdLimitHit was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show snmp user-table

show snmp user-table

Description

Displays the list of SNMP user profiles.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp user-table
SNMP USER TABLE
-----
USER      AUTHPROTOCOL  PRIVACYPROTOCOL  FLAGS
-----
Sam       SHA           AES
fire      SHA           AES
```

The output of this command includes the following parameters:

Parameter	Description
auth-prot	Authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.
priv-prot	Privacy protocol for the user, either AES or CBC-DES, and the password for use with the designated protocol.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show spanning-tree

```
show spanning-tree
  <interface [gigabitethernet <slot/module/port> | port-channel id]
  <vlan vlan-id>
```

Description

View the RSTP and PVST+ configuration.

Parameter	Description
interface	Enter the keyword interface followed by the interface and slot/module/port or port-channel id: <ul style="list-style-type: none">■ For Gigabit Ethernet enter the keyword gigabitethernet followed by the <slot/module/port>■ For Port Channel enter the keyword port-channel followed by an id number Range: 0 to 7
vlan	Enter the keyword vlan follow by the VLAN ID. Default: 1 Range: 1 to 4094

Example—show spanning-tree

```
(host) # show spanning-tree

Spanning tree instance for vlan 10
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs

Spanning tree instance for vlan 20
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 3 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 1 days, 0 hours, 3 mins, 2 secs
```

Example—show spanning-tree vlan

```
(host) # show spanning-tree vlan 2
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs
```

Example—show spanning-tree interface gigabitethernet

```
(host) (config-if)#show spanning-tree interface gigabitethernet 0/0/1
Interface FE 1/1 (port 2) in Spanning tree is FORWARDING
Port path cost 19, Port priority 128 Role DISNIGNATED
PortFast DISABLED P-to-P ENABLED
Designated root has priority 0 address 00:01:e8:d5:a3:6d
Designated bridge has priority 32768 address 00:0b:86:50:58:30
Designated port is 2, path cost 0
Timers: message age 0, forward delay 20, hold 0
Counts: BPDUs received 0, sent 0
```

Related Commands

Related Command	Description
ap system-profile	This command configures an AP system profile.
ap wired-port-profile	This command configures a wired port profile.
interface gigabitethernet	This command configures a GigabitEthernet interface.
interface port-channel	This command configures an Ethernet port channel.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show spantree

```
show spantree  
  <blocking> | <enable> | <forwarding> | <off> | <vlan>
```

Description

View the global RSTP and PVST+ topology.

Parameter	Description
blocking	View the spanning tree ports in the Blocking state.
enable	View the spanning tree ports in the Enable state.
forwarding	View the spanning tree ports in the Forwarding state.
off	View the ports with spanning tree disabled
vlan	View the spanning tree instance for the VLAN.

Example

```
(host) # show spantree  
Spanning tree instance      vlan 1  
Designated Root MAC        00:0b:86:6b:57:80  
Designated Root Priority    32768  
Root Cost                   20000  
Root Max Age 20 sec      Hello Time 2 sec      Forward Delay 15 sec  
  
Bridge MAC                  00:1a:1e:00:89:b8  
Bridge Priority             32768  
Configured Max Age 20 sec  Hello Time 2 sec      Forward Delay 15 sec  
  
Rapid Spanning Tree port configuration  
-----  
Port      State      Cost      Prio  PortFast  BpduGuard  P-to-P  Role  
-----  
GE 0/0/0  Forwarding 20000     128   Disable   Disable     Enable  Root  
GE 0/0/1  Discarding 20000     128   Disable   Disable     Enable  Disabled  
GE 0/0/2  Discarding 2000      128   Disable   Disable     Enable  Disabled  
GE 0/0/3  Discarding 2000      128   Disable   Disable     Enable  Disabled  
GE 0/0/4  Discarding 2000      128   Disable   Enable      Enable  Disabled  
GE 0/0/5  Discarding 2000      128   Disable   Disable     Enable  Disabled  
Pc 0      Discarding 2000000   128   Disable   Disable     Enable  Disabled  
Pc 1      Discarding 2000000   128   Disable   Disable     Enable  Disabled  
Pc 2      Discarding 2000000   128   Disable   Disable     Enable  Disabled  
Pc 3      Discarding 2000000   128   Disable   Disable     Enable  Disabled
```

Related Commands

Related Command	Description
ap system-profile	This command configures an AP system profile.
ap wired-port-profile	This command configures a wired port profile.
interface gigabitethernet	This command configures a GigabitEthernet interface.
interface port-channel	This command configures an Ethernet port channel.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show ssh

show ssh

Description

Displays the SSH configuration details.

Example

The output of this command shows SSH configuration details.

```
(host) [mynode] #show ssh
SSH Settings:
-----
DSA                               Enabled
Mgmt User Authentication Method    username/password public-key
Ciphers                            aes128-cbc,aes256-cbc,aes128-ctr,aes192-
ctr,aes256-ctr
MACs                               hmac-sha1-96,hmac-sha1,hmac-sha2-256
KexAlgorithms                     diffie-hellman-group14-sha1,diffie-
hellman-group14-
sha256,diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-
nistp384
(ST61.62) [mynode] #
(ST61.62) [mynode] (config) #ssh disable-mac hmac-sha1 hmac-sha1-96
(ST61.62) ^[mynode] (config) #write mem
Saving Configuration...
Configuration Saved.
(ST61.62) [mynode] (config) #
(ST61.62) [mynode] (config) #show running-config | include ssh
Building Configuration...
netsservice svc-ssh tcp 22
ssh mgmt-auth public-key
ssh mgmt-auth username/password
ssh disable-mac hmac-sha1-96,hmac-sha1
id "_sftp-ssh._tcp"
id "_ssh._tcp"
```

Related Commands

Command	Description
ssh	Configures SSH access to a Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>KexAlgorithms</code> parameter was added. .
ArubaOS 8.7.0.0	The <code>hmac-sha2-256</code> parameter was added.
ArubaOS 8.3.0.0	The following parameters were added: <ul style="list-style-type: none"> ▪ <code>ssh disable-ciphers</code> ▪ <code>ssh disable-mac</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show sso idp-profile

```
show sso idp-profile
```

Description

Displays all SSO IDP profiles.

No parameters.

Example

The output of this command lists all SSO IDP profiles on the controller.

```
((host) (config) #show sso idp-profile
SSO Profile List
-----
Name           References  Profile Status
----           -
sso-example 0
```

Related Commands

Command	Description
sso idp-profile	This command configures an SSO Identity Provider profile for use with application SSO with L2 Authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show station-table

```
show station-table [mac <mac_address> | verbose ]
```

Description

Displays the internal station table entries and also details of a station table entry.

Parameter	Description
mac <mac_address>	Displays the details of the AP that matches the specified MAC address.
verbose	Displays the details of all the APs in a table format.

Example

The output of this command shows details of an entry in the station table.

```
(host) # show station-table mac 00:1f:6c:7a:d4:fd
Association Table
-----
      BSSID           IP           Essid     AP name   Phy   Age
-----
00:0b:86:6d:3e:30  10.15.20.252  sam      -         a     01:03:41
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show stm

```
show stm
  aruba-death-reasons
  mon-update-queue {stats | threshold}
  perf-history {length | interval}
```

Description

This command is used to display the deauthentication reasons and the monitoring update queue information from the station management module.

Parameter	Description
aruba-death-reasons	Displays the Aruba deauthentication reasons.
mon-update-queue	Displays the STM monitoring update queue information.
stats	Displays the STM update queue statistics.
threshold	Displays the STM monitoring update queue threshold.
perf-history	Displays the association rate history for every five minute of the past 24 hours, by default. Starting from ArubaOS 8.6.0.17 and 8.7.1.9, the output of the show stm perf-history command will display the Avg rate/s to indicate the average number of association requests received by the controller.
duration	Displays the output for the duration specified. Default: 24 hours.
interval	Displays the output for the time interval specified. Default: 5 minutes.

Example

The following command displays the STM deauthentication reasons:

```
(host) [mynode] #show stm aruba-death-reasons
Aruba Death Reasons
-----
Code  Reason
----  -
1     Unspecified Failure
2     Prior authentication is not valid
3     STA has left and is deauthenticated
4     Inactive Timer expired and STA was disassociated
5     Disassociated due to insufficient resources at AP
```

```

6     Class 2 frames from non authenticated STA
7     Class 3 frames from non associated STA
8     STA has left and is disassociated
9     STA Requesting Association without authentication
...
...
..

```

The following command displays the STM monitoring queue update statistics:

```

(host) [mynode] #show stm mon-update-queue stats
(host) [mynode] #show stm mon-update-queue stats
Stm mon update queue statistics
Mon queue size:0
AP Devices Queued
-----
Add   Info Update   Delete   Stats Update
---   -
0     0             0        0
AP Devices Dropped
-----
Add   Info Update   Delete   Stats Update
---   -
0     0             0        0
RADIO Devices Queued
-----
Add   Info Update   Delete   Stats Update
---   -
0     0             0        0
...
...

```

The following command displays the monitoring update queue threshold value:

```

(host) [mynode] #show stm mon-update-queue threshold
Stm mon update queue limit:83328

```

The following command displays the number of association requests received by the controller for the past 24 hours.

```

((host) #show stm perf-history
Association Rate History
-----
Day   Hour   Min   Total   Peak rate/s   Peak time
---   ---   ---   ---
10    14     45    5725    40.0           14:47:34
10    14     50    9850    40.0           14:50:26
10    14     55    10040   40.0           14:55:05
10    15     0     9860    40.0           15:01:30
10    15     5     9900    40.0           15:05:18

```

```

10 15 10 9900 40.0 15:10:33
10 15 15 9900 40.0 15:15:16
10 15 20 10075 40.0 15:20:05

```

Related Commands

Command	Description
stm	This command is used to manually disconnect a client from an AP or control the blacklisting/denylisting of clients.

Command History

Release	Modification
ArubaOS 8.6.0.16	interval and duration parameters are added to the show stm perf-history command.
ArubaOS 8.10.0.0	The <code>mon-update-queue {stats threshold}</code> parameter was deprecated.
ArubaOS 8.6.0.17 and 8.7.1.9	The output parameter Avg rate/s has been added to the show stm perf-history command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show stm-timing-stats

```
show stm-timing-stats
```

Description

This command shows STM/SAPM timing measurements.

No parameters.

Example

The following command displays the STM/SAPM timing measurements,

```
(host)[mynode] #show stm-timing-stats
Wed May 1 23:56:47 2019
STM Stats
handle_nanny_message: calls=2 tot=0 avg=0 min=9 max=16 hist=[0 0 0 0 0 0 0 0
0 0 ]
stm_sapm_process_cmd: calls=1 tot=252637 avg=252637000 min=252637547
max=252637547 hist=[0 0 0 0 0 0 0 0 1 ]
SAPM Stats
Dispatcher Stats
f=0x7f62ab8239b0 calls=0 avg/total/min/max=0/0/0/0 hist=[0 0 0 0 0 0 0 0 0
]
f=0x7f62ab8239b0 calls=0 avg/total/min/max=0/0/0/0 hist=[0 0 0 0 0 0 0 0 0
]
f=0x7f62ab8239b0 calls=0 avg/total/min/max=0/0/0/0 hist=[0 0 0 0 0 0 0 0 0
]
PAPI Stats
f=0x44fe56 calls=3 avg/tot/min/max=0/0/12/18 hist=[0 0 0 0 0 0 0 0 0 0 ]
f=0x44fe56 calls=0 avg/tot/min/max=0/0/0/0 hist=[0 0 0 0 0 0 0 0 0 0 ]
f=0x44fe56 calls=0 avg/tot/min/max=0/0/0/0 hist=[0 0 0 0 0 0 0 0 0 0 ]
Timer Handler Stats
main:1388: calls=14 tot=0 avg=0 min=2 max=19 hist=[0 0 0 0 0 0 0 0 0 0 ]
sapm_ap_mgmt_init:1275: calls=2 tot=0 avg=0 min=2 max=3 hist=[0 0 0 0 0 0 0
0 0 0 ]
wifi_auth_reg_timer_init:11149: calls=2 tot=0 avg=0 min=4 max=13 hist=[0 0 0
0 0 0 0 0 ]
```

The optional output modifiers `| begin`, `| exclude`, and `| include` help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The `| redirect-output` modifier helps you redirect the command output.

Related Commands

Command	Description
stm	This command is used to manually disconnect a client from an AP or control the blacklisting/denylisting of clients.

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show storage

show storage

Description

Displays the storage information on the controller.

No parameters.

Example

The output of this command shows the storage details on the controller.

```
(host) # show storage
Filesystem      Size      Used Available Use% Mounted on
/dev/root       57.0M     54.6M      2.3M   96% /
none            70.0M     2.0M     68.0M    3% /tmp
/dev/hda3       149.7M     9.3M    132.6M    7% /flash
/dev/usb/flash3 1.5G     168.6M    1.3G   12% /flash
/dev/usbdisk/2 3.5G     71.4M     3.2G    2% /mnt/usbdisk/2
/dev/usbdisk/1 3.9G    131.0M     3.8G    3% /mnt/usbdisk/1
```

The number at the end of the USB device's name is the partition. Unlike the controller's flash, the USB device has more than two partitions; not just 0 and 1. When copying a file from a USB device, you must know which partition the target file is on.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show switch ip

```
show switch ip
```

Description

Displays the IP address of the controller and VLAN ID.

No parameters.

Example

The output of this command shows the IP address and VLAN ID of the controller.

```
(host) # show switch ip
Switch IP Address: 10.16.15.1
Switch IP is from Vlan Interface: 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show switch software

```
show switch software
```

Description

Displays the details of the software running in the controller.

No parameters.

Example

The output of this command shows the details of software running in the controller.

```
(host) # show switch software

Aruba Operating System Software.
ArubaOS (MODEL: Aruba6000-US), Version 6.2.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2012, Aruba Networks, Inc.
Compiled on 2012-11-28 at 23:35:56 PST (build 36322) by p4build
ROM: System Bootstrap, Version CPBoot 1.3.0.1 (build 28907)
Built: 2011-06-24 13:46:21
Built by: p4build@re_client_28907
Switch uptime is 15 hours 11 minutes 48 seconds
Reboot Cause: Datapath timeout.
Supervisor Card
Processor XLR 732 (revision C4) with 2015M bytes of memory.
32K bytes of non-volatile configuration memory.
512M bytes of Supervisor Card System flash (model=CF 512MB).
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show switches

```
show switches [all| debug | regulatory | state {complete | incomplete | inprogress  
| required} | summary ]
```

Description

Displays the details of managed device connected to the Mobility Conductor, including the Mobility Conductor itself.

Parameter	Description
all	List of all managed devices.
debug	Displays additional switch information.
regulatory	Displays information about the currently active regulatory file.
state	Configuration status of all managed devices.
summary	Status of all managed devices connected to the Mobility Conductor.

Example

The output of this command shows that there is a single managed device connected to the Mobility Conductor.

```
(host) # show switches all
All Switches
-----
IP Address  Name           Location           Type   Version           Status
Configuration State  Config Sync Time (sec)
-----  ----  -----  ----  -----  -----  --
-----  -----
10.16.12.1  r-wing-94      Building1.floor1  master  6.0.0.0_13782  up
UPDATE SUCCESSFUL  0192.0.2.12  CorpA2400      Building1.floor1  master
6.0.0.0_13782  up          UPDATE SUCCESSFUL  0
```

Execute the `show switches regulatory` command to check if the regulatory file is active on the managed device.

```
(host) #show switches regulatory

All Switches
-----
```

IP Address	Name	Location	Type	Model	File Version
172.16.0.254	host	Building1.floor1	master	7210	1.0_43859
File Build					
21/4/2014					

Execute the `show switches state complete` command to check the progress of the configuration update.

```
(host)[mynode] #show switches state
[incomplete|incomplete|inprogress|required]
(host) [mynode] (config) #show switches state complete
All Switches
-----
IP Address   IPv6 Address   Name           Location        Type  Model
  Version
-----
1.1.1.1     2002::1       abhi_vmc_61.122  Building1.floor1  LC   VMC-
TACTICAL  8.0.0.0-svcs-ctrl_0000

Status       Configuration State  Config Sync Time (sec)  Config ID
-----
up           UPDATE SUCCESSFUL    0                        22
Total Switches:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show switchinfo

```
show switchinfo
```

Description

Displays the latest and complete summary of managed device details including role, last configuration change, hostname, and reason for last reboot.

No parameters.

Example

The output of this command lists all managed devices connected to Mobility Conductor including the Mobility Conductor server.

```
(host) # show switchinfo
Hostname is Techpubs
Console Baudrate: 115200
Location not configured
System Time:Tue Nov 27 16:22:14 PST 2012
        Aruba Operating System Software.

        ArubaOS (MODEL: Aruba7220-US), Version 6.2.0.0
        Website: http://www.arubanetworks.com
        Copyright (c) 2002-2012, Aruba Networks, Inc.

Compiled on 2012-11-26 at 17:06:31 PST (build 36290) by p4build
ROM: System Bootstrap, Version CPBoot 1.2.0.9 (build 35873)
Built: 2012-10-24 13:51:09
Built by: p4build@re_client_35873
Switch uptime is 9 hours 34 minutes 3 seconds
Reboot Cause: User reboot.
Built: 2012-10-24 13:51:0
Built by: p4build@re_client_35873

Internet address is 172.16.0.254 255.255.255.0
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled
Encapsulation 802, loopback not set
Last clearing of "show interface" counters 0 day 9 hr 34 min 3 sec
link status last changed 0 day 9 hr 34 min 3 sec
Proxy Arp is disabled for the Interface
switchrole:master
Configuration unchanged since last save
Crash information available.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show syscontact

show syscontact

Description

Displays the contact information for support.

No parameters.

Example

The output of this command shows the contact information for technical support.

```
(host) # show syscontact  
  
admin@mycompany.com
```

Related Commands

Related Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show syslocation

show syslocation

Description

Displays the location details of the controller.

No parameters.

Example

The output of this command location of the controller.

```
(host) # show syslocation  
Building 1, Floor 1
```

Related Commands

Related Command	Description
ap system-profile	This command configures an AP system profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show tech-support

```
show tech-support
  airgroup
    <filename>
  lte_uplink
    <filename>
  user
```

Description

Displays all information about the controller required for technical support purposes.

Parameter	Description
<code>airgroup</code>	Starting from ArubaOS 8.6.0.5, the command displays AirGroup related tech-support logs.
<code>lte_uplink</code>	Displays all LTE related uplink CLI
<code><filename></code>	Stores the output in specified file name. Maximum length of the file name is 127 characters
<code>user</code>	Run a user specific tech-support command.

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: All instances of <code>master</code> have been replaced with <code>conductor</code> . All instances of <code>blacklist</code> have been replaced with <code>denylist</code> . All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.6.0.5	The <code>airgroup</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show telnet

```
show telnet
```

Description

Displays the status of telnet access using the CLI or Serial over Ethernet (SOE) to the controller.
No parameters.

Example

The output of this command shows the status of CLI and SOE access to the controller.

```
(host) # show telnet  
  
telnet cli is enabled  
telnet soe is enabled
```

Related Commands

Related Command	Description
telnet	This command enables telnet to Mobility Conductor or to an AP through Mobility Conductor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show threshold

show threshold

all | controlpath-cpu | controlpath-memory | datapath-cpu |
no-of-aps | no-of-locals | no-of-vaps | total-tunnel-capacity | user-capacity |

Description

This command shows managed device capacity thresholds which, when exceeded, will trigger alerts.

Parameter	Description
all	Display all alert thresholds.
controlpath-cpu	Display the alert threshold for controlpath CPU capacity. The output of this command shows the percentage of the total controlpath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 45%.
controlpath-memory	Display the alert threshold for controlpath memory consumption. The output of this command shows the percentage of the total memory capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 85%.
datapath-cpu	Display the alert threshold for datapath CPU capacity. The output of this command shows the percentage of the total datapath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 30%.
no-of-APs	The maximum number of APs that can be connected to a managed device is determined by that managed device's model type and installed licenses. This threshold triggers an alert when the number of APs currently connected to the managed device exceeds a specific percentage of its total AP capacity. The default threshold for this parameter is 80%.
no-of-locals	Display the alert threshold for Mobility Conductor's capacity to support managed devices. Mobility Conductor can support a combined total of 256 managed devices. The output of this command shows the percentage of the total Mobility Conductor capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

Parameter	Description
no-of-vaps	The maximum number of VAPs that can be connected to a managed device is determined by that managed device's model type and installed licenses. This threshold triggers an alert when the number of VAPs currently connected to the managed device exceeds a specific percentage of its total VAP capacity. The default threshold for this parameter is 80%.
total-tunnel-capacity	Display the alert threshold for the managed device's tunnel capacity. The output of this command shows the percentage of the managed device's total tunnel capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%
user-capacity	Display the alert threshold for the managed device's user capacity. The output of this command shows the percentage of the total resource capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

The managed device will send a *wlsxThresholdAbove* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdBelow* SNMP trap and error message will be triggered if the resource usage drops below the threshold once again.

Example

```
(host) (config) #show threshold all
controller Capacity Threshold Values
-----
RESOURCE                THRESHOLD (%)
-----
Datapath-Cpu             30 %
Controlpath-Cpu         80 %
Controlpath-Memory      85 %
Total-Tunnel-Capacity   80 %
Ap-Tunnel-Capacity      80 %
User-Capacity           80 %
No-of-APs               80 %
No-of-locals            80 %
```

Related Commands

Command	Description
aaa authentication captive-portal	This command configures a Captive Portal authentication profile.

Command	Description
aaa authentication wispr	This command configures WISPr authentication with the WISPr RADIUS server of an ISP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show threshold-limits

show threshold-limits

```
controlpath-memory| fan-speed| no-of-aps| no-of-locals| no-of-vaps| total-tunnel-  
capacity| user-capacity
```

Description

This command shows current values of the different resources monitored by the managed device.

Parameter	Description
controlpath-memory	The output of this command displays the default memory threshold which, when exceeded, will trigger an alert, the current configured threshold, the total memory (in MB) and the currently available memory (in MB).
fan-speed	The output of this command displays the fan alert threshold. This parameter is only available for managed devices with fans, such as the 7200 Series.
no-of-aps	The output of this command displays the following values: <ul style="list-style-type: none">▪ The default threshold for the number of APs, which, when exceeded, will trigger an alert▪ The current configured threshold.▪ The maximum number of APs supported by the managed device,▪ The number of available licenses for campus and remote APs,▪ The total number of APs, and the current number of campus, remote and virtual APs.
no-of-locals	The output of this command displays the default threshold for the number of managed devices which, when exceeded, will trigger an alert, and the current configured threshold. The output also displays the maximum number of managed devices that can be connected to this Mobility Conductor, and the number of managed devices currently connected.
no-of-vaps	The output of this command displays the following values: <ul style="list-style-type: none">▪ The default threshold for the number of Virtual APs, which, when exceeded, will trigger an alert▪ The current configured threshold.▪ The maximum number of Virtual APs supported by the managed device,▪ The total number of current Virtual APs.

Parameter	Description
<code>total-tunnel-capacity</code>	The output of this command displays the default tunnel capacity threshold which, when exceeded, will trigger an alert, as well as the current configured tunnel threshold. The output also includes the maximum number of tunnels supported by the managed device, as well as the number of tunnels currently used by the managed device.
<code>user-capacity</code>	The output of this command displays the default user capacity threshold which, when exceeded, will trigger an alert, as well as the current configured user threshold. The output also includes the maximum number of users supported by the managed device, as well as the number of users currently associated with the managed device.

The managed device will send a *wlsxThresholdAbove* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdBelow* SNMP trap and error message will be triggered if the resource usage drops below the threshold once again.

Example

The following command shows the current alert thresholds for controlpath memory resources:

```
[host](node)(config) #show threshold-limits controlpath-memory

Threshold Values For Controlpath Memory
-----
Default(%)   Current(%)   Total Memory (MB)   Available Memory (MB)
-----
85           77           679                 225
```

Related Commands

Command	Description
vrrp	This command configures the VRRP.
uplink	This command manages and configures the uplink network connection.

Command History

Release	Modification
ArubaOS 8.6.0.0	The <code>no-of-vaps</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show time-range

```
show time-range [<name>|summary]
```

Description

Displays the list of time range configured in the system and rules affected by the time range.
No parameters.

Example

The output of this command shows the absolute time range details.

```
(host) # show time-range

Time-Range monitoring, Absolute
-----
StartDate  Start-time  EndDate      End-time     Applied
-----
4/29/2009  23:00       4/30/2009   12:00       No
```

Related Commands

Command	Description
time-range	This command configures time ranges.
time-range-profile	This command configures time range profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show timer debug statistics app-name

show timer debug statistics app-name <name>

Description

Display timer debugging statistics for a specific application.

Parameter	Description
<name>	<p>One of the following application names:</p> <ul style="list-style-type: none">▪ aaa: Administrator Authentication▪ ads: Anomaly Detection▪ authmgr: User Authentication▪ certmgr: Certificate Manager▪ cfgm: Config Manager▪ cluster_mgr: Cluster Manager▪ cluster_upgrade_mgr: Cluster Upgrade Manager▪ cpsec: Control-Plane Security Manager▪ cts: Transport Service▪ dbsync: Database Synchronization▪ dhcp: DHCP Server▪ esi: Server Load Balancing▪ fpapps: Layer 2,3 control▪ ha_mgr: HA manager▪ httpd: HTTPD▪ ike: IKE Daemon▪ l2tp: L2TP▪ licensemgr: License Manager▪ mdns: AirGroup mdns▪ mobileip: Mobile IP▪ ntp: NTP Daemon▪ off-loader: Off-Loader▪ ospf: OSPF▪ pim: Protocol Independent Multicast▪ pktfilter: Packet Filter▪ pptp: PPTP▪ profmgr: Profile Manager▪ publisher: Publish subscribe service▪ resolver: Resolver▪ snmp: SNMP agent▪ stm: Station Management▪ syslogd: Syslog Manager▪ tunneled_node_mgr : Tunneled Node Manager▪ userdb: User Database Server

Parameter	Description
	<ul style="list-style-type: none"> ▪ web_cc: Web Content Classification ▪ wms: Wireless Management ▪ wpa3_sae: SAE Parent process

Example

The following example shows IPC statistics for the **STM** process.

```
(host) #show timer debug statistics app-name stm

Granularity=100
Wheel Size=512
Tick Count=5744522
Spoke Index=394
Active timers=21
Expired timers=886374
Hiwater mark=49
Started timers=109893
Cancelled timers=4425
Timer info
SI      TV      RC      Recurring      RT      Callback      FN
0       3600000 30      Yes            1575400 0x2ad41c84    PAPI_Init_
Prio:1245
0       3600000 30      Yes            1575400 0x2ad4a200    PAPI_Init_
Prio:1249
0       3600000 30      Yes            1575400 0x2ad41c84    PAPI_Init_
Prio:1245
0       3600000 30      Yes            1575400 0x2ad4a200    PAPI_Init_
Prio:1249
0       3600000 30      Yes            1575400 0x2ad41c84    PAPI_Init_
Prio:1245
0       3600000 30      Yes            1575400 0x2ad4a200    PAPI_Init_
Prio:1249
0       3600000 30      Yes            1575400 0x2ad41c84    PAPI_Init_
Prio:1245
0       3600000 30      Yes            1575400 0x2ad4a200    PAPI_Init_
Prio:1249
0       3600000 30      Yes            1575400 0x2ad41c84    PAPI_Init_
Prio:1245
0       3600000 30      Yes            1575400 0x2ad4a200    PAPI_Init_
Prio:1249
360    300000  0      Yes            3400     0x57d564      sapm_ap_mgmt_
init:831
360    60000  0      Yes            3400     0x46942c
addservicetomonitor:169
360    60000  0      Yes            3400     0x2b230730    Nanny_Start_
Processing:98
360    60000  0      Yes            3400     0x54e8a4      voip_ucm_
init:255
```

```

380  60000  0      No      1400  0x646fb8  mon_mgr_set_
coll_stats_timer:48
402  1000  0      Yes     800  0x42a068  main:1104
410  300000 1      Yes    52800 0x5b599c  sapm_gap_read_
db:3409
422  5000  0      Yes     2800  0x2b2544a0  boc_licusage_
init:115
447  8085  0      No      5300  0x478660  mux_
heartbeat:1017
472  10000 0      Yes     7800  0x41ce70  wifi_auth_reg_
timer_init:7539
492  60000  0      No      9800  0x42a820  stm_set_net_
stats_update_timer:
SI: Spoke Index TV: Timer Value RC: Rotation Count
RT: Remaining Time      FN: Function:Line Number

```

Related Commands

Command	Description
time-range	This command configures time ranges.
time-range-profile	This command configures time range profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show tm

```
show tm
  mon-update-queue {stats | threshold}
```

Description

This command is used to display the monitoring update queue information of the telemetry manager module.

Parameter	Description
mon-update-queue	Displays the TM monitoring update queue information.
stats	Displays the TM update queue statistics.
threshold	Displays the TM monitoring update queue threshold.

Example

The following command displays the TM monitoring queue update statistics:

```
(host) [mynode] #show tm mon-update-queue stats
Telemetry-Manager MON update queue statistics
Mon queue size:0
Mon queue threshold:3334
Mon queue current percentage of threshold:0%
Mon queue timer:stopped
TM MON Stats (Queued/Dropped)
-----
MON Device  Add  Update Info  Update Stats  Delete
-----
NETWORK    1   0           1632          0
AP          10  13          4783          8
RADIO      17   0           6478          12
VAP        21   0           6478          12
STA         1/0  1/0         1544/0        0
USER        1/0  8/0          0/0           0
IP_USER     4/0  0/0          0/0           0
DENYLIST    0   0            0             0
```

The following command displays the monitoring update queue threshold value:

```
(host) [mynode] #show tm mon-update-queue threshold
Telemetry-Manager MON update queue limit:3334
0: disabled
```

Related Commands

Command	Description
tm	This command is used to configure the maximum queue size for the TM monitoring updates.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show tpm

```
show tpm
  cert-info
  errorlog
  version
```

Description

Displays the TPM and factory certificate information and error log.

Use this command to verify that TPM and factory certificates are installed as expected.

Parameter	Description
cert-info	Displays the factory certificate information.
errorlog	Displays the TPM/certificate related error logs.
version	Displays the TPM firmware version information.

Example

In the example below, the TPM and certificates are installed.

```
(host) [mynode] #show tpm cert-info

subject= /CN=AF0000168::00:0b:86:f0:33:e0
issuer= /DC=com/DC=arubanetworks/DC=ca/CN=DEVICE-CA2
serial=1F023F05000000015087
notBefore=Jan 30 01:38:57 2009 GMT
notAfter=Jan 25 01:38:57 2029 GMT
```

In the example below, the controller is unable to verify the TPM or factory certificate information.

```
(host) [mynode] #show tpm cert-info

Cannot get TPM and Factory Certificate Info
TPM and/or Factory Certificates might be missing.
```

In the example below, the TPM initialization errors are displayed.

```
(host) [mynode] #show tpm errorlog
```

```

05032018:15:30:25>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:30:25>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:30:34>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:30:34>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:30:44>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:30:44>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:30:54>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:30:54>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:30:54>>ERROR>>TPM Setup at System Initialization failed
05032018:15:31:03>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:31:03>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:31:13>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:31:13>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:31:23>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:31:23>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:31:32>>ERROR>>TPM LoadKey Command failed with return code
(0x00000006)
05032018:15:31:32>>ERROR>>TpmLoadKey Failed for Certified Key
05032018:15:31:32>>ERROR>>TPM Setup at System Initialization failed
05032018:15:31:32>>ERROR>>TPM or Device Cert Initialization failed.
05032018:15:31:40>>ERROR>>Error while opening /tmp/tpmKeyHandles.bin for
reading TPM Handles,errno(2)
05032018:15:31:40>>ERROR>>FindTpmKeyHandle for key ID 0x00000002 failed
05032018:15:32:39>>ERROR>>Error getting Intermediate Certificates for the
device
05032018:15:33:23>>ERROR>>Error while opening /tmp/tpmKeyHandles.bin for
reading TPM Handles,errno(2)
05032018:15:33:23>>ERROR>>FindTpmKeyHandle for key ID 0x00000002 failed
05032018:15:33:23>>ERROR>>TpmDecryptWithKeyId failed to decrypt with TPM key
2 in function DecryptFieldSymKeyWithTPM.
05032018:15:33:23>>ERROR>>For purpose 15, error decrypting
/flash/config/fieldCerts/15/symKey.bin.enc to
/tmp/fieldPrivKeys/symKey.bin.15 with TPMEncKEY_ID=2 failed.
05032018:15:33:23>>ERROR>>Error decrypting private key(s).
05032018:15:33:23>>ERROR>>Error decrypting field private key(s). Please
check if the flash is corrupted.
05032018:15:33:23>>ERROR>>Field Cert Initialization failed.

```

Related Commands

Command	Description
zeroize-tpm-keys	This command is used to erase the TPM content and render a controller permanently inoperable.

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>errorlog</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable Mode

show trunk

```
show trunk
```

Description

Displays the list of trunk ports on the controller.

No parameters.

Example

The output of this command shows details of a trunk port.

```
(host) # show trunk

Trunk Port Table
-----
Port      Vlans Allowed          Vlans Active
         Native Vlan
-----
FE2/12    1, 613, 615-617, 632-633, 636-640, 667-668  1, 613, 615-617, 632-633, 636-640, 667-668  1
```

Related Commands

Command	Description
interface port-channel	This command configures an Ethernet port channel.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed device.

show tunnel-group

show tunnel-group <tunnel-group-name>

Description

Displays the operational status of the tunnel-groups configured on the controller.

Parameter	Description
<tunnel-group-name>	Displays the operational status of the specified tunnel-group.

Example

The output of this command shows the status of the configured tunnel-groups:

```
(host) #show tunnel-group

Tunnel-Group Table Entries
-----
Tunnel Group Type Tunnel Group Id Preemptive Failover Active Tunnel Id
Tunnel Members
-----
tgroup1      L3   16385          enabled           10             10
20
tgroup2      L2   16387          enabled           10             10
20 40
```

The output of the following command shows the status of the specified tunnel-group:

```
(host) #show tunnel-group tgroup1

Tunnel-Group Table Entries
-----
Tunnel Group Type Tunnel Group Id Preemptive Failover Active Tunnel Id
Tunnel Members
-----
tgroup1      L3   16385          enabled           10             10
20
```

The output of the following command shows the datapath Tunnel-Group table entries:

```
(host) #show datapath tunnel-group

Datapath Tunnel-Group Table Entries
```

```

-----
Tunnel-Group Active Tunnel Members
-----
16385          10          10 20

```

Related Commands

Command	Description
tunnel-group	This command creates a tunnel-group to group a set of tunnels.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show tunneled-node

```
show tunneled-node {config|state|database}
```

Description

Displays the wired tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Parameter	Description
config	Displays the wired tunneled node configuration details.
state	Displays the state of the tunneled node.
database	Displays all the tunneled nodes in the database.

Example

The output of this command shows the tunneled node state.

```
(host) [mynode]# show tunneled-node state

Tunneled Node State
-----
IP MAC s/p state vlan tunnel inactive-time
-- -- -- -- -- -- --
192.168.123.14 00:0b:86:40:32:40 1/23 complete 10 9 1
192.168.123.14 00:0b:86:40:32:40 1/22 complete 10 10 1
192.168.123.14 00:0b:86:40:32:40 1/20 complete 10 11 1
```

On the tunneled node client:

```
(host) #show tunneled-node state

Tunneled Node State
-----
IP          MAC          s/p  state  vlan  tunnel  inactive-
time
--          ---          ---  -----  ---  -----  -----
192.168.123.16 00:0b:86:40:32:40 1/23 complete 10 21 0
192.168.123.16 00:0b:86:40:32:40 1/22 complete 10 9 0
```

Related Commands

Command	Description
tunneled-node-address	This command configures the IP address of a tunneled node server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show tunneled-node-mgr

show tunneled-node-mgr

Description

Displays the tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Parameter	Description
cluster-bucket-map	Displays the cluster bucket map details.
cluster-node-list	Displays the cluster node list information.
gsm-counters	Displays the GSM counters details.
mcast-tunnel-table	Information on multicast tunnel.
mcast-vlan-user-map	Information on the user count on each multicast tunnel VLAN pair.
node-heartbeat-table	Displays node heartbeat table related information.
stats	Displays the tunneled node manager statistics.
trace-buf	Displays contents of trace buffer.
tunnel-vlan-user-map	Displays Information on user count on each Tunnel VLAN pair.
tunneled-nodes	Displays all the information on tunneled nodes.
tunneled-users	Displays all the information on tunneled users.
user-tunnel-table	Displays information on user tunnel tables.

Example

You can use the following show command to check if the per-user tunnel node is configured and is working as expected.

```
(host) [mynode]# show tunneled-node-mgr stats

Message stats
-----
Switch bootstrap
```

```
-----  
switch_bootstrap_req: 2  
switch_bootstrap_req_fail_mandatory_param_absent: 0  
switch_bootstrap_req_fail_invalid_key: 0  
switch_bootstrap_req_fail_actv_req_on_stby_ctrl: 0  
switch_bootstrap_req_fail_stby_req_on_actv_ctrl: 0  
switch_bootstrap_req_fail_not_actv_or_stby: 0  
switch_bootstrap_req_fail_hbt_tunnel_creation_fail: 0  
switch_bootstrap_req_fail_wait_for_license_response: 1  
switch_bootstrap_req_fail_license_not_received: 0  
switch_bootstrap_req_fail_platform_limit_reached: 0  
switch_bootstrap_ack_fail_bmap_not_present: 0  
switch_bootstrap_ack: 1  
switch_bootstrap_nack: 0
```

Switch unbootstrap

```
-----  
switch_unbootstrap_msg: 0  
switch_unbootstrap_msg_fail_switch_not_found: 0  
switch_unbootstrap_msg_fail_not_actv_or_stby: 0  
switch_unbootstrap_ack: 0  
switch_unbootstrap_nack: 0
```

Switch failover

```
-----  
switch_failover_msg: 0  
switch_failover_msg_fail_mandatory_param_absent: 0  
switch_failover_msg_fail_switch_not_found: 0  
switch_failover_msg_fail_switch_actv: 0  
switch_failover_msg_fail_ctrl_not_stby: 0  
switch_failover_ack: 0  
switch_failover_nack: 0
```

User bootstrap

```
-----  
user_bootstrap_req: 3  
user_bootstrap_req_fail_mandatory_param_absent: 0  
user_bootstrap_mac_move_switch_mac_differs: 0  
user_bootstrap_mac_move_user_key_differs: 0  
user_bootstrap_req_fail_invalid_key: 0  
user_bootstrap_req_fail_bmap_mismatch: 0  
user_bootstrap_req_fail_tunnel_creation_fail: 0  
user_bootstrap_req_fail_auth_entry_creation_fail: 0  
user_bootstrap_ack: 3  
user_bootstrap_nack: 0
```

User unbootstrap

```
-----  
user_unbootstrap_msg: 1  
user_unbootstrap_msg_fail_mandatory_param_absent: 0  
user_unbootstrap_msg_fail_switch_mismatch: 0  
user_unbootstrap_msg_fail_key_mismatch: 0  
user_unbootstrap_msg_fail_user_not_found: 0  
user_unbootstrap_msg_fail_switch_not_found: 0  
user_unbootstrap_ack: 1  
user_unbootstrap_nack: 0
```

Switch keepalive

switch_keep_alive: 0
switch_keep_alive_fail_switch_not_found: 0
switch_keep_alive_ack: 0
switch_keep_alive_nack: 0

Nodelist message

node_list_send_fail_switch_bootstrap_not_acked: 0
node_list_send_fail_switch_max_attempt: 0
node_list_message: 4
node_list_ack_switch_not_found: 0
node_list_ack_invalid_seq_num: 0
node_list_ack: 4
node_list_resend: 0

Bucketmap message

bucket_map_send_fail_switch_bootstrap_not_acked: 1
bucket_map_send_fail_switch_max_attempt: 0
bucket_map_message: 1
bucket_map_ack_switch_not_found: 0
bucket_map_ack_invalid_seq_num: 0
bucket_map_ack: 1
bucket_map_resend: 0

Cluster stats

Cluster object

no_slot_for_new_node: 0
cluster_object_add: 4
cluster_object_disconnect: 6
down_node_not_found: 6
cluster_disable_events: 0

Cluster sac

stby_sac_removements: 0
inform_switch_sac_down: 0
ignore_sby_sac_switch_not_found: 0
skip_sby_sac_on_sby: 0
sby_sac_updates_sent: 1

Bucketmap

bmap_event_but_cluster_disabled: 0
bmap_create_events: 1
bmap_update_events: 1
bmap_errors: 0
bmap_del_mapped_dormant_sta: 0
bmap_del: 0
self_not_in_bmap: 0

```

User activation
-----
activations: 0
activation_errors: 0
sta_not_dormant: 0
uac_down_activate_bmap: 0
activation_fail_down_uac_not_in_bmap: 0
activation_fail_self_not_in_bmap: 0

User dormant creation
-----
sta_dormant_add_switch_not_found: 0
sta_dormant_add_sta_creation_failed: 0
sta_dormant_add_sta_add_to_bucket: 0
sta_dormant_add_tunnel_updated: 0
sta_dormant_add_tunnel_creation_failed: 0

User dormant deletion
-----
dormant_del: 0
dormant_del_sta_not_active: 0
dormant_del_sta_not_dormant: 0
station_not_found: 0

Add standby switch to ndoelist
-----
stby_sac_switch_add: 0
stby_sac_switch_del: 0

In memory
-----
add_switch: 1
del_sta_from_sta_hash: 1
add_sta: 0
add_dormant_sta_to_switch: 0
add_sta_to_switch: 3
sta_hash_not_found_in_switch: 0
sta_removed_from_switch: 1
deauth_sta: 1
deauth_all_sta: 0
delete_switch: 0

```

Related Commands

Command	Description
tunnel-group	This command creates a tunnel-group to group a set of tunnels.

Command History

Release	Modification
ArubaOS 8.4.0.0	The following parameters were added: <ul style="list-style-type: none"> ▪ <code>mcast-tunnel-table</code> ▪ <code>mcast-vlan-user-map</code>
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config modes on managed devices.

show uap-blacklist/show uap-denylist

show uap-blacklist / show uap-denylist [mac-address|page|start]

Description

This command configures a UAP blacklist/denylist database entry. You can add, delete, or modify AP MAC addresses and description to this database. If you enable the blacklist/denylist policy in the AP deploy profile, the policy is applied to the APs included in this list.

Parameter	Description
mac-address <name>	Shows MAC address of the AP.
page	Shows specific page (50 records per page).
start	Shows <start> records into the database

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following commands lists all the AP MAC addresses in the UAP blacklist/denylist table:

```
(host) [mynode] #show uap-blacklist/show uap-denylist
UAP Blacklist /Denylist Details
-----
MAC-Address      Description
-----
11:11:11:11:11:11 AP-test2
11:11:11:11:11:12 Ap-test1
11:11:11:11:11:01 AP-test3
```

Related Commands

Command	Description
uap-blacklist / uap-denylist	This command allows you to create or purges the UAP blacklist/denylist database by adding, deleting, or modifying AP MAC address entries.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show ucc

```
show ucc
  call-info
  client-info
  custom-sip
  dns-ip-learning
  facetime
  h323
  ich
  internal-state
  jabber
  noe
  rtpa-config
  rtpa-report
  sccp
  session-idle-timeout
  sip
  skype4b
  statistics
  teams
  trace-buffer
  vocera
  webrtc
  wificalling
```

Description

This command shows the active UCC configuration. Click parameter links to view the corresponding show commands.

Parameter	Description
call-info	Shows ucc call detailed records (CDRs).
client-info	Shows ucc client status and record.
custom-sip	Shows the custom-sip ALG Configuration.
dns-ip-learning	Shows the ePDG IP addresses.
facetime	Shows the FaceTime ALG Configuration.
h323	Shows the H323 ALG Configuration.
ich	Shows the Intelligent Call Handling Configuration.
internal-state	Shows UCC internal-state information.

Parameter	Description
jabber	Shows the Jabber ALG Configuration.
noe	Shows the NOE ALG Configuration.
rtpa-config	Shows the Real-Time Analysis Configuration.
rtpa-report	Shows Real-Time Analysis report.
sccp	Shows the SCCP ALG Configuration.
session-idle-timeout	Shows the UCC Session Idle Timeout Configuration.
sip	Shows the SIP ALG Configuration.
skype4b	Shows the Skype4B ALG Configuration.
statistics	Shows UCC statistics.
teams	Shows the Microsoft Teams ALG configuration.
trace-buffer	Shows call trace buffer.
vocera	Shows the Vocera ALG Configuration.
webrtc	Shows the WebRTC ALG Configuration.
wificalling	Shows the WiFi Calling Configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc client-info

```
show ucc client-info
  app
    {h323 [detail]|jabber [detail]|noe [detail]|sccp [detail]|sip [detail]|skype4b
    [detail]|svp [detail] | vocera [detail]|WiFi-Calling [detail]}
  detail
  sta <mac>
```

Description

This command displays the UCC client status and CDR statistics.



When VoIP calls are prioritized using media classification, the **Client Name** value is not available.

Parameter	Description
app	Displays the UCC client status and CDR statistics based on a specific ALG.
detail	Displays UCC client status details.
sta <mac>	Displays the detailed record for a specific client based on its MAC address.

Example

The following command displays the UCC client status and record:

```
(host) [mynode] #show ucc client-info

Client Status:
-----
Client IP      Client MAC      Client Name  ALG      Server (IP)
Registration State Call Status
-----
-----
192.0.2.22    00:23:33:41:c8:b8  Alex        SIP      192.0.2.1
REGISTERED      Idle
192.0.2.26    24:77:03:9a:6c:dc  John        Jabber   192.0.2.3
REGISTERED      Idle

AP Name  Flags  Device Type  Home Agent  Foreign Agent
-----
AP-105   OS X   OS X         192.0.2.25  NA
AP-135   Win 7  Win 7         192.0.2.25  NA

Total Client Entries:2
```

Flags: V - Visitor, A - Away, W - Wired, R - Remote, E - External

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.
Server (IP)	Displays the IP address of call server the client is registered to.
Registration State	Displays the registration status of the VoIP call. Possible values are: <ul style="list-style-type: none">▪ Challenged▪ Registered▪ Registering▪ Unregistered▪ Rejected▪ Unknown
Call Status	Displays the VoIP call status of the client. Possible values are: <ul style="list-style-type: none">▪ Idle▪ In-Call
AP Name	Displays the name of the AP to which the VoIP client is associated.
Flags	Displays if the client is a visitor, away, wired, remote, or external.
Device Type	Displays the device type identification of the client.
Home Agent	Displays the IP address of the managed device to which the client is connected or the home agent of the client if mobile IP is enabled.
Foreign Agent	Displayed if the client has roamed to another managed device when mobile IP is enabled.

The following command displays the UCC client status details:

```
(host) [mynode] #show ucc client-info detail
```

```

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End
      D - Delay in milliseconds
      J - Jitter in milliseconds
      PL - Packet Loss in percent

Client Status Details(Average):
-----
Client IP      Client MAC      Client Name      Controller Delay(ms)/Jitter
(ms)/PktLoss(%)
-----
192.0.2.22    00:23:33:41:c8:b8  Alex            1.33/0.15/1.99
192.0.2.26    24:77:03:9a:6c:dc  John            0.82/0.17/0.05

AP Delay(ms)/Jitter(ms)/PktLoss(%)  End-to-End Delay(ms)/Jitter(ms)/PktLoss
(%)  Call-Dur(sec)  TxRate(Mbps)  RxRate(Mbps)
-----
1.04/0.09/2.26                        79.00/3.23/1.72
   1114                        84.42      130.56
1.12/0.15/2.63                        10.36/3.55/0.07
   584                        27.02      30.12

ICH Denied  ALG
-----
0           SIP
0           Jabber

Total Client Entries:2

```

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
Controller Delay(ms) / Jitter(ms) / PktLoss(%)	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the managed device.
AP Delay(ms) / Jitter(ms) / PktLoss(%)	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the AP.

Column	Description
End-to-End Delay (ms) / Jitter (ms) / PktLoss (%)	Displays the end-to-end delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This field takes the wired and wireless network QoS parameters into consideration.
Call-Dur (sec)	Displays the average call duration in seconds.
TxRate (Mbps)	Displays the average transmission rate in Mbps.
RxRate (Mbps)	Displays the average receive rate in Mbps.
ICH Denied	Displays the number of calls that were not prioritized due to channel utilization threshold exceeding on the AP radio.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.

The following command displays a detailed record for a specific client MAC address:

```
(host) [mynode] #show ucc client-info sta 00:21:6a:b9:5f:34

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP

Station Report:
-----
Client IP      Client MAC      AP-Name  SNR  Avg Tx Rate (Mbps)
-----
10.15.88.245  00:21:6a:b9:5f:34  AP-135-1  45   54.56

Tx Drop (%)   Tx Retry (%)   Avg Rx Rate (Mbps)   Rx Retry (%)   Un-steerable
(reason)
-----
1.06          24.06         43.16                0.41          NA

Active Calls:
-----
CDR ID  UCC Call ID  Client IP      Client Name  ALG      Dir  Called To  Dur
(sec)   Orig-Time
-----
116     12           10.15.88.245  Alex        skype4b  OG   Joe        421
      Jan 20 01:36:08

Status  Call Type  Client Health  UCC Score[C]  UCC Score[A]  MOS
-----
ACTIVE  Voice     62             81.52/Good    83/01Good     4.17/Good

Call History:
-----
```

```

CDR ID  UCC Call ID  Client IP      Client Name  ALG      Dir  Called To  Dur
(sec)   Orig-Time
-----  -
54      23              10.15.88.245  Alex        skype4b  OG   Mike       847
      Jan 16 02:45:22
53      22              10.15.88.245  Alex        skype4b  OG   Ken        789
      Jan 14 06:53:41

Status Reason      Call Type      Client Health  UCC Score[C]  UCC Score
[A]  MOS
-----  -
SUCC  Terminated  Voice          49             71.72/Good    73.99/Good
      3.85/Good
SUCC  Terminated  Voice/Conf Call 44             77.22/Good    79.01/Good
      4.13/Good

```

The output of this command includes the following information:

Column	Description
Station Report	
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
AP-Name	Displays the name of the AP handling the VoIP call.
SNR	Displays the Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Avg Tx Rate (Mbps)	Displays the average transmission rate in Mbps.
Tx Drop (%)	Displays the transmission packet drop in percentage.
Tx Retry (%)	Displays the transmission retry in percentage.
Avg Rx Rate (Mbps)	Displays the average receive rate in Mbps.
Rx Retry (%)	Displays the receive retry in percentage.
Un-steerable (reason)	Displays the reason for steering/not steering the client to another band. Possible values are: <ul style="list-style-type: none"> ▪ Sticky ▪ Load Balance ▪ Band Steer

Column	Description
	<ul style="list-style-type: none"> ▪ Band Balance ▪ Administrator Added ▪ (IOS) ▪ NA
Active Calls	
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session.
Client IP	Displays the IP address of the VoIP client.
Client Name	Displays the username of the VoIP client.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.
Dir	Displays the direction of the call. Possible values are: <ul style="list-style-type: none"> ▪ OG—Outgoing ▪ IG—Incoming
Called To	Displays the username of the VoIP client being called.
Dur (sec)	Displays the duration of the VoIP call in seconds.
Orig-Time	Displays the time at which the VoIP call originated.
Status	Displays the status of the VoIP call. Possible values are: <ul style="list-style-type: none"> ▪ SUCCESS ▪ FAILED ▪ ABORTED ▪ BLOCKED ▪ FORWARDED ▪ ALERTING ▪ HOLD ▪ ACTIVE
Call Type	Displays the type of VoIP call or session. Possible values are: <ul style="list-style-type: none"> ▪ Not Available ▪ Voice ▪ Video ▪ Desktop Sharing ▪ File Transfer ▪ Voice/Conf Call ▪ Video/Conf Call

Column	Description
	<ul style="list-style-type: none"> ▪ Desktop-Sharing/Conf Call ▪ File-Transfer/Conf Call
Client Health	Displays the ratio of ideal air time required for transmitting a packet from an AP to a client to the actual air time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.
UCC Score[C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.
UCC Score[A]	Displays the UCC score based on the quality of the voice call or desktop sharing session. This is the metric calculated at the AP.
MOS	Displays the Mean Opinion Score of the VoIP call.
Call History	
Reason	<p>Displays the reason code for call termination. Possible values are:</p> <ul style="list-style-type: none"> ▪ NA ▪ Capacity Reached ▪ 401 unauthorized ▪ 487 request timeout ▪ Request timeout ▪ Request canceled ▪ Request terminated ▪ Session timeout ▪ Session timer expired ▪ Session expired - request timeout ▪ Aborted ▪ Terminated ▪ Forwarded ▪ Transferred ▪ Inactivity ▪ Wrong number ▪ Peer reset ▪ Client reset ▪ No answer ▪ Missed ▪ Parked ▪ Invalid number ▪ Tunnel down ▪ Moved temporarily ▪ 4xx error ▪ 5xx error

Column	Description
	<ul style="list-style-type: none"> ▪ Call leg does not exist ▪ DELTS request ▪ TCLAS flow deleted ▪ No reason
<p>NOTE: For information on additional field descriptions, refer the field descriptions under the Active Calls heading.</p>	

Related Commands

Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc custom-sip

show ucc custom-sip

Description

This command displays the custom SIP ALG configuration.

No parameters.

Example

The following command displays the custom SIP ALG configuration:

```
(host) [mynode] #show ucc custom-sip

custom SIP ALG Configuration
-----
Parameter          Value
-----
SIP ALG Support    Enabled
app-name           test
key-name           ConnectVoice
voice priority     34
video priority     48
custom-sip-port    55060
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc dns-ip-learning

show ucc dns-ip-learning

Description

This command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device. This command is specific for Wi-Fi calling clients.

No parameters.

Example

The following command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device:

```
((host) [mynode] #show ucc dns-ip-learning

DNS IP Learning:
-----
IP Address      Service Provider
-----
208.54.85.108   T-Mobile
208.54.73.77    T-Mobile
208.54.70.110   T-Mobile
208.54.77.253   T-Mobile
208.54.75.2     T-Mobile
208.54.85.64    T-Mobile
208.54.73.76    T-Mobile
208.54.83.96    T-Mobile
208.54.85.111   T-Mobile

Total Entries:9
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc facetime

```
show ucc facetime
```

Description

This command displays the Apple Facetime ALG configuration.

No parameters.

Example

The following command displays the Apple Facetime ALG configuration:

```
(host) [mynode] #show ucc facetime

FaceTime ALG Configuration
-----
Parameter                Value      Set
-----                -
FaceTime ALG Support     Enabled
video priority           34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc h323

```
show ucc h323
```

Description

This command displays the H.323 ALG configuration.

No parameters.

Example

The following command displays the H.323 ALG configuration:

```
(host) [mynode] #show ucc h323

H323 ALG Configuration
-----
Parameter          Value      Set
-----
H323 ALG Support   Enabled
voice priority     46
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc ich

```
show ucc ich
```

Description

This command displays the Intelligent Call Handling configuration.
No parameters.

Example

The following command displays the Intelligent Call Handling configuration:

```
(host) [mynode] #show ucc ich

Intelligent Call Handling Configuration
-----
Parameter                               Value      Set
-----
Intelligent Call Handling                Enabled
Channel Utilization Threshold           90
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc internal-state

```
show ucc internal-state
```

Description

This command displays the number of CDRs, flows, and voice clients created. This is a debug command.

No parameters.

Example

The following command displays the UCM internal state statistics:

```
(host) [mynode] #show ucc internal-state

UCM Internal State Statistics
-----
Clients      Active CDRs   Ended CDRs   Flows Installed   Flows Agedout   VC
creation failed
-----
3            0             43           140                13              0

Clients (Last)  Flows Installed (Last)  Flows AgedOut (Last)  VC creation
failed (Last)
-----
0              0                     0                      0
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc jabber

show ucc jabber

Description

This command displays the Cisco Jabber ALG configuration.

No parameters.

Example

The following command displays the Cisco Jabber ALG configuration:

```
(host) [mynode] #show ucc jabber

Jabber ALG Configuration
-----
Parameter                Value          Set
-----                -
Jabber ALG Support       Enabled
Jabber server ip         192.0.2.2
Jabber server ip         192.0.2.3
voice priority            46
video priority            34
app-sharing priority      34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc noe

```
show ucc noe
```

Description

This command displays the Alcatel-Lucent New Office Environment (NOE) ALG configuration. No parameters.

Example

The following command displays the Alcatel-Lucent NOE ALG configuration:

```
(host) [mynode] #show ucc noe

NOE ALG Configuration
-----
Parameter          Value      Set
-----
NOE ALG Support    Enabled
voice priority     46
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc rtpa-config

```
show ucc rtpa-config
```

Description

This command displays the real-time analysis configuration.

No parameters.

Example

The following command displays the real-time analysis configuration:

```
(host) [mynode] #show ucc rtpa-config

Real-Time Analysis Configuration
-----
Parameter                               Value      Set
-----
Real-Time Analysis of VoIP calls         Enabled
Upstream Real-Time Analysis of VoIP calls Enabled
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc rtpa-report

show ucc rtpa-report

Description

This command displays the real-time analysis report.

Example

The following command displays the real-time analysis report:

```
(host) [mynode] #show ucc rtpa-report

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End

Real-Time Analysis Call Quality Report
-----
Client (IP)      Client (MAC)      Client (Name)  ALG  Jitter(usec) [C]  Pkt-
loss (%) [C]    Delay(usec) [C]
-----
192.168.201.240  f0:7b:cb:3b:65:5c  1002          SIP  23.700
0.000           101.800
192.168.201.246  00:24:d7:40:a8:58  1003          SIP  30.912
0.000           257.140

UCC Score[C]    Jitter(usec) [A]  Pkt-loss (%) [A]  Delay(usec) [A]  UCC Score[A]
Forward mode
-----
68.366          0.000             0.499             316.400          84.119
decrypt-tunnel
82.551          0.000             0.000             327.478          85.999
decrypt-tunnel

Num Records:2
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc sccp

```
show ucc sccp
```

Description

This command displays the Cisco Skinny Client Control Protocol (SCCP) ALG configuration.

Example

The following command displays the Cisco SCCP ALG configuration:

```
(host) [mynode] #show ucc sccp

SCCP ALG Configuration
-----
Parameter          Value      Set
-----
SCCP ALG Support   Enabled
voice priority     46
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc session-idle-timeout

```
show ucc session-idle-timeout
```

Description

This command displays the UCC session idle timeout configuration.

Example

The following command displays the UCC session idle timeout configuration:

```
(host) [mynode] #show ucc session-idle-timeout

UCC Session Idle Timeout Configuration
-----
Parameter                Value  Set
-----
UCC Session Idle Timeout  35
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc sip

show ucc sip

Description

This command displays the SIP ALG configuration.

Example

The following command displays the SIP ALG configuration:

```
(host) [mynode] #show ucc sip

SIP ALG Configuration
-----
Parameter                Value      Set
-----                -
SIP ALG Support           Enabled
SIP Midcall request timeout Disabled
RTCP Inactivity           Disabled
voice priority            46
video priority            34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc skype4b

show ucc skype4b

Description

This command displays the Skype4B ALG configuration.

Example

The following command displays the Skype4B ALG configuration:

```
(host) [mynode] #show ucc skype4b

Skype4B ALG Configuration
-----
Parameter                Value      Set
-----                -
Skype4B ALG Support      Enabled
Skype4B SDN Over http/https https
voice priority           46
video priority           34
app-sharing priority     34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc statistics

```
show ucc statistics counter call
  client [app {h323|jabber|noe|sccp|sip|skype4b|svp|vocera|WiFi-Calling}]
  global [app {h323|jabber|noe|sccp|sip|skype4b|svp|vocera|WiFi-Calling}]
```

Description

This command displays the UCC call statistics.

Parameter	Description
client	Displays per client call statistics counter.
global	Displays system-wide call statistics counter.

Example

The following command displays the global call counters:

```
(host) [mynode] #show ucc statistics counter call global

System-wide Call Counters:
-----
Call Originated  Call Terminated  Active  Success  Failed  Blocked
-----
6                37                0       12       29      0

Aborted  Forwarded  WMM AC-VI  WMM AC-VO  WMM-BK  WMM-BE
-----
2        0        6         0         0       8

Device Type Allocations:
-----
Device Type  WMM AC-VI  WMM AC-VO  WMM-BK  WMM-BE
-----
Win 7        0          0         0       6
Apple        3          0         0       0
OS X         3          0         0       0

WMM (VI, VO, BK, BE):total calls with received priority
The following command displays the client call counters:
(host) [mynode] #show ucc statistics counter call client

Per Client Call Counters:
-----
Client IP      Client MAC      Call Originated  Call Terminated  Active
Success  Failed
-----
-----
```

```

10.15.88.216 10:40:f3:82:91:04 0          32          0          3
  29
10.15.88.217 10:40:f3:82:c1:48 3          0          0          3
  0
10.15.88.245 00:26:c6:52:6b:7c 2          4          0          4
  0
10.15.88.218 00:21:6a:b9:5f:34 1          1          0          2
  0

Blocked   Aborted   Forwarded   WMM AC-VI   WMM AC-VO   WMM-BK   WMM-BE
-----
0         0         0           3           0           0         0
0         0         0           3           0           0         0
0         2         0           0           0           0         6
0         0         0           0           0           0         2

WMM (VI, VO, BK, BE):total calls with received priority

```

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Call Originated	Displays the number of times a call originated from the VoIP client.
Call Terminated	Displays the number of times a call terminated on the VoIP client.
Active	Displays the number of active calls on the VoIP client.
Success	Displays the number of successful calls.
Failed	Displays the number of failed call setup calls.
Blocked	Displays the number of blocked calls due to CAC.
Aborted	Displays the number of terminated calls due to inactivity.
Forwarded	Displays the number of times a call is forwarded for a VoIP client.
WMM AC-VI	Displays the number of calls where the client sent RTP with WMM AC set to Video (VI).
WMM AC-VO	Displays the number of calls where the client sent RTP with WMM AC set to Voice (VO).

Column	Description
WMM-BK	Displays the number of calls where the client sent RTP with WMM AC set to Background (BK).
WMM-BE	Displays the number of calls where the client sent RTP with WMM AC set to Best Effort (BE).

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc teams

```
show ucc teams
```

Description

This command displays the Microsoft Teams ALG configuration.

Example

The following command displays the Microsoft Teams ALG configuration:

```
(host) [mynode] #show ucc teams

MS-Teams ALG Configuration
-----
Parameter                Value
-----
MS-Teams ALG Support     Enabled
voice priority           46
video priority           34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.8.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc trace-buffer

```
show ucc trace-buffer
  jabber [count <0-65535>]
  sccp [count <0-65535>]
  sip [count <0-65535>]
  skype4b[count <0-65535>]
```

Description

This command displays the UCC call message trace buffer for Cisco Jabber, Cisco SCCP, SIP, and Microsoft Skype for Business ALGs. Call signaling events such as establishing voice, video, desktop sharing, and file transfer are recorded.

Parameter	Description
jabber [count <0-65535>]	Displays the Jabber call message trace buffer.
sccp [count <0-65535>]	Displays the SCCP call message trace buffer.
sip [count <0-65535>]	Displays the SIP call message trace buffer.
skype4b [count <0-65535>]	Displays the Skype4b call message trace buffer.

Example

The following command displays Skype4b call message trace buffer:

```
(host) #show ucc trace-buffer skype4b

Skype4b Voice Client(s) Message Trace
-----
Client IP      Client MAC      Client Name     Direction     Event Time
BSSID
-----
---
192.0.2.22     00:23:33:41:c8:b8  Alex           OG            Jan  3 11:24:34
9c:1c:12:8a:b5:50
192.0.2.26     24:77:03:9a:6c:dc  John           OG            Jan  3 11:24:34
9c:1c:12:8a:b5:50
192.0.2.29     00:22:90:ea:9e:f1  Steve          OG            Jan  3 11:24:08
9c:1c:12:8a:b5:50

Called To      Media Type      AP Name        Src Port      Dest Port      Call Status
-----
Joe            Voice/Video     AP-225         50030/58008   50032/58006   Start of call
Mike            Voice/Video     AP-225         50032/58008   50030/58008   InCallQuality
Update
```

```
Ken      Voice      AP-225  50026    50038    Call Quality
Update

Num of Rows:3
```

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the user name of the VoIP client.
Direction	Displays the call direction. <ul style="list-style-type: none"> ▪ OG — Outgoing ▪ IC — Incoming
Event Time	Displays the time stamp when the VoIP call originated.
BSSID	Displays the BSSID of the AP to which the VoIP client is connected.
Called To	Displays the user name of the VoIP client being called.
Media Type	Displays the type of Skype4b call. This can be one of the following: <ul style="list-style-type: none"> ▪ Desktop-sharing ▪ File-transfer ▪ Video ▪ Voice
AP Name	Displays the name of the access point receiving calls.
Src Port	Displays the source port for the media session.
Dest Port	Displays the destination port of the particular media session.
Call Status	Displays if the Skype4b client is in any one of the following call status: <ul style="list-style-type: none"> ▪ Start of call ▪ End of call ▪ Before call update ▪ Call Quality Update ▪ InCallQuality Update ▪ After call update

Related Commands

Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc vocera

```
show ucc vocera
```

Description

This command displays the Vocera ALG configuration.

Example

The following command displays the Vocera ALG configuration:

```
(host) [mynode] #show ucc vocera

Vocera ALG Configuration
-----
Parameter           Value
-----
Vocera ALG Support  Enabled
voice priority      46
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc webrtc

```
show ucc webrtc
```

Description

This command displays the webRTC ALG configuration.

Example

The following command displays the custom SIP ALG configuration:

```
(host) [mynode] #show ucc webrtc

WebRTC ALG Configuration
-----
Parameter           Value
-----
WebRTC ALG Support  Enabled
voice priority      46
video priority      34
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc wificalling

```
show ucc wificalling
```

Description

This command displays the Wi-Fi calling configuration.

Example

The following command displays the Wi-Fi calling configuration:

```
(host) [mynode] [mynode] #show ucc wificalling

WiFi Calling Configuration
-----
Parameter                Value
-----
WiFi Calling Support      Enabled
voice priority            46
dns pattern               N/A
```

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc call-info cdrs

```
show ucc call-info cdrs
  ap <ap_name>
  app
  cid <cid>
  detail
```

Description

This command displays the Call Detailed Records (CDR) statistics for Unified Communication and Collaboration (UCC). Click parameter links to view the corresponding show commands.



When VoIP calls are prioritized using media classification, the **UCC Call ID**, **Client Name**, **Called to**, **Dir** (direction of the call), **End-to-End Delay(ms)/Jitter(ms)/PktLoss(%)**, **Codec**, **MOS**, and **MOS-Band** values are not available.

Parameter	Description
ap <ap_name>	Displays the CDR statistics of an AP for a specific Application Layer Gateway (ALG).
app	Displays the CDR statistics based on a specific ALG.
cid <cid>	Displays CDR statistics for a specific CDR-ID.
detail	Displays detailed CDR statistics.

Example

The following command displays the CDR statistics:

```
(host) [mynode] #show ucc call-info cdrs

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP

CDRS:
-----
CDR ID  UCC Call ID  Client IP      Client MAC      Client Name  ALG
Dir
-----
---
43      12            192.0.2.22    00:23:33:41:c8:b8  Alex         skype4b
  IC
42      12            192.0.2.26    24:77:03:9a:6c:dc  John         skype4b
  OG
```



```

1          NA          10.15.132.86 fc:c2:de:6c:01:9c NA          WiFi-
Calling NA

Called to  Dur(sec)  Orig Time          Status Reason          Call Type
Client Health
-----
-----
-----
-----
-----
-----
Joe        50          Jan  8 06:18:27  SUCC   Terminated  Video/Conf Call
81
Mike       50          Jan  8 06:18:27  SUCC   Terminated  Voice
82
NA         88          Jun  4 06:41:40  ACTIVE NA          Voice
93

UCC Score[C]  UCC- Score[A]  MOS          Server (IP)
-----
-----
-----
-----
81.52/Good   79.18/Good     4.17/Good
79.53/Good   76.24/Good     4.15/Good
NA           NA             NA           T-Mobile

Total Entries:3

```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG.
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client. NOTE: This column is not populated for WiFi-Calling ALG.
ALG	Displays the VoIP protocol used by the VoIP client.
Dir	Displays the direction of the call. Possible values are: <ul style="list-style-type: none"> ▪ OG—Outgoing ▪ IC—Incoming NOTE: This column is not populated for WiFi-Calling ALG.

Column	Description
Called to	Displays the username of the VoIP client being called. NOTE: This column is not populated for WiFi-Calling ALG.
Dur (sec)	Displays the duration of the VoIP call in seconds.
Orig Time	Displays the time at which the VoIP call originated.
Status	Displays the status of the VoIP call. Possible values are: <ul style="list-style-type: none"> ▪ SUCCESS ▪ FAILED ▪ ABORTED ▪ BLOCKED ▪ FORWARDED ▪ ALERTING ▪ HOLD ▪ ACTIVE
Reason	Displays the reason code for call termination. Possible values are: <ul style="list-style-type: none"> ▪ NA ▪ Capacity Reached ▪ 401 unauthorized ▪ 487 request timeout ▪ Request timeout ▪ Request canceled ▪ Request terminated ▪ Session timeout ▪ Session timer expired ▪ Session expired - request timeout ▪ Aborted ▪ Terminated ▪ Forwarded ▪ Transferred ▪ Inactivity ▪ Wrong number ▪ Peer reset ▪ Client reset ▪ No answer ▪ Missed ▪ Parked ▪ Invalid number ▪ Tunnel down ▪ Moved temporarily ▪ 4xx error ▪ 5xx error

Column	Description
	<ul style="list-style-type: none"> ▪ Call leg does not exist ▪ DELTS request ▪ TCLAS flow deleted ▪ No reason
Call Type	<p>Displays the type of VoIP call or session. Possible values are:</p> <ul style="list-style-type: none"> ▪ Not Available ▪ Voice ▪ Video ▪ Desktop Sharing ▪ File Transfer ▪ Voice/Conf Call ▪ Video/Conf Call ▪ Desktop-Sharing/Conf Call ▪ File-Transfer/Conf Call
Client Health	<p>Displays the ratio of ideal air time required for transmitting a packet from an AP to a client to the actual air time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.</p>
UCC Score[C]	<p>Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
UCC Score[A]	<p>Displays the UCC score based on the quality of the voice call or desktop sharing session. This is the metric calculated at the AP.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
MOS	<p>Displays the Mean Opinion Score (MOS) of the VoIP call.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
Server (IP)	<p>Displays the name of the service provider for WiFi-calling ALG</p>

Related Commands

Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.2.0.0	Column Server(IP) is added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc call-info cdrs ap

show ucc call-info cdrs ap <ap_name>

Description

This command displays the Call Detailed Records (CDR) statistics for an AP.

Example

The following command displays the CDR statistics for an AP.

```
(host) [mynode] #show ucc call-info cdrs ap AP225-1

CDR-AP:
-----
CDR ID  UCC Call ID  AP Name  Re-Assoc  ICH-Denied  Utilization(%)  Codec
Quality  Delay(msec)
-----  -----
18      7              AP225-1  0          No           37              G711
Good    0.74
17      7              AP225-1  0          No           37              G711
Fair    19.00
16      6              AP225-1  1          No           34              NA
Good    0.55

Jitter(msec)  Packet Loss(%)  Orig WMM-AC
-----
0.21           0.00            NA
0.37           14.93           0
0.05           0.00            0

Max Concurrent Calls: 3 At Jan 14 03:54:15
Total Entries:3
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG

Column	Description
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
ICH-Denied	Displays the status of the Intelligent Call Handling (ICH). Possible values are: <ul style="list-style-type: none"> ▪ Yes—Call prioritized ▪ No—Call not prioritized
Utilization(%)	Displays the channel utilization of the AP during the call.
Codec	Displays the compression protocol used for voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG
Quality	Displays the quality of the VoIP call based on the UCC score. Possible values are: <ul style="list-style-type: none"> ▪ Good ▪ Fair ▪ Poor ▪ NA NOTE: This column is not populated for WiFi-Calling ALG.
Delay (msec)	Displays the average delay in milliseconds. NOTE: This column is not populated for WiFi-Calling ALG.
Jitter (msec)	Displays the average jitter in milliseconds. NOTE: This column is not populated for WiFi-Calling ALG.
Packet Loss(%)	Displays the loss of packet in percentage. NOTE: This column is not populated for WiFi-Calling ALG.
Orig WMM-AC	Displays the original client value of the Wi-Fi Multimedia Access Category.

Related Commands

Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.2.0.0	Column Server(IP) is added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc call-info cdrs app

```
show ucc call-info cdrs app
  customsip
  facetime
  h323
  jabber
  noe
  sccp
  sip
  skype4B
  svp
  vocera
  webrtc
  WiFi-Calling
```

Description

This command displays the applications list for which you can filter the Call Detailed Records (CDR) statistics. Following are the list of applications.

Parameter	Description
customsip	Filter on Custom-sip.
facetime	Filter on Facetime.
h323	Filter on h323.
jabber	Filter on jabber.
noe	Filter on noe.
sccp	Filter on sccp.
sip	Filter on sip.
skype4B	Filter on skype4B.
svp	Filter on svp.
vocera	Filter on vocera.
webrtc	Filter on WebRTC.
WiFi-Calling	Filter on WiFi-Calling.

Example

The following command displays the CDR statistics filtered on Custom-sip.

```
(host) [mynode] #show ucc call-info cdrs app customsip
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to
Dur(sec)  Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]
UCC Score[A]  MOS  Server(IP)
-----  -----  -----  -----  -----  ---  ---  -----
-----  -----  -----  -----  -----  ---  ---  -----
-----  ---  -----
```

The following command displays the CDR statistics filtered on Facetime.

```
(host) [mynode] #show ucc call-info cdrs app facetime
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to
Dur(sec)  Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]
UCC Score[A]  MOS  Server(IP)
-----  -----  -----  -----  -----  ---  ---  -----
-----  -----  -----  -----  -----  ---  ---  -----
-----  ---  -----
Total Entries:0
```

The following command displays the CDR statistics filtered on h323.

```
(host) [mynode] #show ucc call-info cdrs app h323
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to
Dur(sec)  Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]
UCC Score[A]  MOS  Server(IP)
-----  -----  -----  -----  -----  ---  ---  -----
-----  -----  -----  -----  -----  ---  ---  -----
-----  ---  -----
Total Entries:0
```

The following command displays the CDR statistics filtered on Jabber.

```
(host) [mynode] #show ucc call-info cdrs app jabber
```



```

CDR ID   UCC Call ID   Client IP   Client MAC   Client Name   ALG   Dir   Called to
Dur(sec) Orig Time   Status   Reason   Call Type   Client Health   UCC Score[C]
UCC Score[A]   MOS   Server(IP)
-----
-----
-----
Total Entries:0

```

The following command displays the CDR statistics filtered on skype4B.

```

(host) [mynode] #show ucc call-info cdrs app skype4B
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID   UCC Call ID   Client IP   Client MAC   Client Name   ALG   Dir   Called to
Dur(sec) Orig Time   Status   Reason   Call Type   Client Health   UCC Score[C]
UCC Score[A]   MOS   Server(IP)
-----
-----
-----
Total Entries:0

```

The following command displays the CDR statistics filtered on svp.

```

(host) [mynode] #show ucc call-info cdrs app svp
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID   UCC Call ID   Client IP   Client MAC   Client Name   ALG   Dir   Called to
Dur(sec) Orig Time   Status   Reason   Call Type   Client Health   UCC Score[C]
UCC Score[A]   MOS   Server(IP)
-----
-----
-----
Total Entries:0

```

The following command displays the CDR statistics filtered on teams.

```

(host) [mynode] #show ucc call-info cdrs app teams
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
CDR:
----
CDR ID   UCC Call ID   Client IP   Client MAC   Client Name   ALG   Dir   Called to
Dur(sec) Orig Time   Status   Reason   Call Type   Client Health   UCC Score[C]
UCC Score[A]   MOS   Server(IP)

```

```
-----  
-----  
-----  
Total Entries:0
```

The following command displays the CDR statistics filtered on vocera.

```
(host) [mynode] #show ucc call-info cdrs app vocera  
Help: [C] - Metric calculated at the Controller  
[A] - Metric calculated at the AP  
CDR:  
-----  
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to  
Dur(sec) Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]  
UCC Score[A]  MOS  Server(IP)  
-----  
-----  
-----  
Total Entries:0
```

The following command displays the CDR statistics filtered on webrtc.

```
(host) [mynode] #show ucc call-info cdrs app webrtc  
Help: [C] - Metric calculated at the Controller  
[A] - Metric calculated at the AP  
CDR:  
-----  
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to  
Dur(sec) Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]  
UCC Score[A]  MOS  Server(IP)  
-----  
-----  
-----  
Total Entries:0
```

The following command displays the CDR statistics filtered on vocera.

```
(host) [mynode] #show ucc call-info cdrs app wifi-calling  
Help: [C] - Metric calculated at the Controller  
[A] - Metric calculated at the AP  
CDR:  
-----  
CDR ID  UCC Call ID  Client IP  Client MAC  Client Name  ALG  Dir  Called to  
Dur(sec) Orig Time  Status  Reason  Call Type  Client Health  UCC Score[C]  
UCC Score[A]  MOS  Server(IP)  
-----  
-----  
-----  
Total Entries:0
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
ICH-Denied	Displays the status of the Intelligent Call Handling (ICH). Possible values are: <ul style="list-style-type: none"> ▪ Yes—Call prioritized ▪ No—Call not prioritized
Utilization (%)	Displays the channel utilization of the AP during the call.
Codec	Displays the compression protocol used for voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG
Quality	Displays the quality of the VoIP call based on the UCC score. Possible values are: <ul style="list-style-type: none"> ▪ Good ▪ Fair ▪ Poor ▪ NA NOTE: This column is not populated for WiFi-Calling ALG.
Delay (msec)	Displays the average delay in milliseconds. NOTE: This column is not populated for WiFi-Calling ALG.
Jitter (msec)	Displays the average jitter in milliseconds. NOTE: This column is not populated for WiFi-Calling ALG.
Packet Loss (%)	Displays the loss of packet in percentage. NOTE: This column is not populated for WiFi-Calling ALG.
Orig WMM-AC	Displays the original client value of the Wi-Fi Multimedia Access Category.

The following command displays detailed CDR statistics.

```
(host) [mynode] #show ucc call-info cdrs detail

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End
      D - Delay in milliseconds
      J - Jitter in milliseconds
      PL - Packet Loss in percent

CDR-Detail:
-----
CDR ID  UCC Call ID  AP Name  Re-Assoc  UCC Score[C]  D(ms)/J(ms)/PL(%) [C]
-----
29      11           AP135-1  0          82.70         0.57/0.01/0.42
22      9            AP135-1  0          83.93         0.30/0.00/0.00

21      9            AP135-1  0          85.07         0.33/0.00/0.64

UCC Score[A]  D(ms)/J(ms)/PL(%) [A]  SNR  Avg Tx Rate (Mbps)  Tx Drop(%)  Tx
Retry(%)
-----
81.34         0.68/0.01/0.53         48   45.19               0.27        23.99
82.01         0.45/0.00/0.10         46   532.39              0.00        1.42
84.76         0.52/0.00/0.79         53   58.79               57.52       10.30

Avg Rx Rate (Mbps)  Rx Retry(%)  MOS  D(ms)/J(ms)/PL(%) [E]  Controller-IP
-----
53.70               0.01         3.50  12.58/05.70/05.16      192.0.2.1
355.00              0.01         2.64  10.16/03.81/03.24      192.0.2.1
107.92              0.01         4.07  11.24/04.92/04.18      192.0.2.1

Total Entries:3
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG.

Column	Description
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
UCC Score [C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.
D (ms) / J (ms) / PL (%) [C]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the managed device.
UCC Score [A]	Displays the UCC score based on the quality of the voice call or desktop sharing. This is the metric calculated at the AP. NOTE: This column is not populated for WiFi-Calling ALG.
D (ms) / J (ms) / PL (%) [A]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the AP.
SNR	Displays the Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Avg Tx Rate (Mbps)	Displays the average transmission rate in Mbps.
Tx Drop (%)	Displays the transmission packet drop in percentage.
Tx Retry (%)	Displays the transmission retry in percentage.
Avg Rx Rate (Mbps)	Displays the average receive rate in Mbps.
Rx Retry (%)	Displays the receive retry in percentage.
MOS	Displays the MOS value of the VoIP call. This is an end-to-end score (wired and wireless) of the VoIP call. NOTE: This column is not populated for WiFi-Calling ALG.
D (ms) / J (ms) / PL (%) [E]	Displays the end-to-end delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This field takes the wired and wireless network QoS parameters into consideration.
Controller-IP	Displays the IP address of the managed device.

Related Commands

Command	Description
UCC	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.2.0.0	Column Server(IP) is added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show ucc call-info cdrs cid

show ucc call-info cdrs cid <cid>

Description

This command displays the Call Detailed Records (CDR) statistics for a specific CDR-ID.

Example

The following command displays the CDR statistics for a CDR-ID 201:

```
(host) [mynode] #show ucc call-info cdrs cid 201
Help: [C] - Metric calculated at the Controller
[A] - Metric calculated at the AP
[E] - Metric calculated End-to-End
D - Delay in milliseconds
J - Jitter in milliseconds
PL - Packet Loss in percent
CDR-Basic:
-----
CDR ID   UCC Call ID   Client IP       Client MAC       Client Name      ALG
  Dir   Called to   Dur(sec)   Orig Time       Status   Reason          Call Type
-----
201     NA           10.20.104.3   40:b0:76:6c:6f:cc Client         WiFi-
Calling NA    NA           33           Oct 27 19:39:04 SUCC      Terminated
Voice
Session-Details:
-----
Src IP       Src Port   Dst IP       Dst Port   Codec   DSCP   Orig-DSCP   WMM-AC
Orig WMM-AC
-----
10.20.104.3 41393     49.44.59.38 4500       NA      46     60          6
7
AP Quality-Details:
-----
AP Name           Re-Assoc   UCC Score[A]   Avg Delay(msec)   Avg Jitter
(msec)   Avg Packet Loss(%)   Avg Tx Rate(Mbps)   Tx Drop(%)   Tx Retry(%)   Avg
Rx Rate(Mbps)   Rx Retry(%)
-----
SH-GF-ALPHA-P27-HW-03 0           NA             NA              NA              NA
NA              NA              NA              NA              NA
NA
Controller Quality-Details:
-----
UCC Score[C]   Avg Delay(msec)   Avg Jitter(msec)   Avg Packet Loss(%)
-----
NA              NA              NA              NA
```

```

End-to-End Quality-Details:
-----
MOS   Avg Delay(msec)   Avg Jitter(msec)   Avg Packet Loss(%)
-----
NA    NA                NA                 NA
Events:
-----
Timestamp          AP Name                BSSID                Category   Event
-----
Oct 27 19:39:08   SH-GF-ALPHA-P27-HW-03  a8:bd:27:ed:c8:40   Handoff   Joining
AP
Oct 27 19:39:08   SH-GF-ALPHA-P30-APLAB  90:4c:81:6a:4f:60   Handoff   Leaving
AP
Call Samples(per 60 secs):
-----
Timestamp          Client Health   UCC Score[C]   D(ms)/J(ms)/PL(%) [C]   UCC
Score[A]   D(ms)/J(ms)/PL(%) [A]   SNR   Avg Tx Rate(Mbps)   Tx Drop(%)   Tx Retry
(%)   Avg Rx Rate(Mbps)   Rx Retry(%)   MOS   End-to-End D(ms)/J(ms)/PL(%)
Event
-----
Oct 27 19:39:37   0                NA                NA/NA/NA                NA
NA/NA/NA                NA                NA                NA
NA                NA                NA                NA/NA/NA                NA
Oct 27 19:39:08   0                NA                NA/NA/NA                NA
NA/NA/NA                NA                NA                NA
NA                NA                NA                NA/NA/NA                Handoff
(L2)
Oct 27 19:39:08   0                NA                NA/NA/NA                NA
NA/NA/NA                NA                NA                NA
NA                NA                NA                NA/NA/NA                NA

```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG.
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client. NOTE: This column is not populated for WiFi-Calling ALG.

Column	Description
ALG	Displays the VoIP protocol used by the VoIP client.
Dir	Displays the direction of the call. Possible values are: <ul style="list-style-type: none"> ▪ OG—Outgoing ▪ IC—Incoming NOTE: This column is not populated for WiFi-Calling ALG.
Called to	Displays the username of the VoIP client being called. NOTE: This column is not populated for WiFi-Calling ALG.
Dur (sec)	Displays the duration of the VoIP call in seconds.
Orig Time	Displays the time at which the VoIP call originated.
Status	Displays the status of the VoIP call. Possible values are: <ul style="list-style-type: none"> ▪ SUCCESS ▪ FAILED ▪ ABORTED ▪ BLOCKED ▪ FORWARDED ▪ ALERTING ▪ HOLD ▪ ACTIVE
Reason	Displays the reason code for call termination. Possible values are: <ul style="list-style-type: none"> ▪ NA ▪ Capacity Reached ▪ 401 unauthorized ▪ 487 request timeout ▪ Request timeout ▪ Request canceled ▪ Request terminated ▪ Session timeout ▪ Session timer expired ▪ Session expired - request timeout ▪ Aborted ▪ Terminated ▪ Forwarded ▪ Transferred ▪ Inactivity ▪ Wrong number ▪ Peer reset ▪ Client reset

Column	Description
	<ul style="list-style-type: none"> ▪ No answer ▪ Missed ▪ Parked ▪ Invalid number ▪ Tunnel down ▪ Moved temporarily ▪ 4xx error ▪ 5xx error ▪ Call leg does not exist ▪ DELTS request ▪ TCLAS flow deleted ▪ No reason
Call Type	<p>Displays the type of VoIP call or session. Possible values are:</p> <ul style="list-style-type: none"> ▪ Not Available ▪ Voice ▪ Video ▪ Desktop Sharing ▪ File Transfer ▪ Voice/Conf Call ▪ Video/Conf Call ▪ Desktop-Sharing/Conf Call ▪ File-Transfer/Conf Call
Client Health	<p>Displays the ratio of ideal air time required for transmitting a packet from an AP to a client to the actual air time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.</p>
UCC Score[C]	<p>Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
UCC Score[A]	<p>Displays the UCC score based on the quality of the voice call or desktop sharing session. This is the metric calculated at the AP.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
MOS	<p>Displays the Mean Opinion Score (MOS) of the VoIP call.</p> <p>NOTE: This column is not populated for WiFi-Calling ALG.</p>
Server (IP)	<p>Displays the name of the service provider for WiFi-calling ALG</p>

Command History

Release	Modification
ArubaOS 8.2.0.0	Column Server(IP) is added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. NOTE: This column is not populated for WiFi-Calling ALG.
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
UCC Score[C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.
D (ms) / J (ms) / PL (%) [C]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the managed device.
UCC Score[A]	Displays the UCC score based on the quality of the voice call or desktop sharing. This is the metric calculated at the AP. NOTE: This column is not populated for WiFi-Calling ALG.
D (ms) / J (ms) / PL (%) [A]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the AP.
SNR	Displays the Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Avg Tx Rate (Mbps)	Displays the average transmission rate in Mbps.
Tx Drop (%)	Displays the transmission packet drop in percentage.
Tx Retry (%)	Displays the transmission retry in percentage.
Avg Rx Rate (Mbps)	Displays the average receive rate in Mbps.
Rx Retry (%)	Displays the receive retry in percentage.
MOS	Displays the MOS value of the VoIP call. This is an end-to-end score (wired and wireless) of the VoIP call. NOTE: This column is not populated for WiFi-Calling ALG.

Column	Description
D (ms) / J (ms) / PL (%) [E	Displays the end-to-end delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This field takes the wired and wireless network QoS parameters into consideration.
Controller-IP	Displays the IP address of the managed device.

Related Commands

Command	Description
ucc	This command configures the various UCC Application Layer Gateways (ALGs).

Command History

Release	Modification
ArubaOS 8.2.0.0	Column Server(IP) is added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config or Enable mode on Mobility Conductor.

show upgrade internal

```
show upgrade internal managed-devices status
  copy list <mac-list>
  reboot list <mac-list>
  summary list <mac-list>
```

Description

This command displays the upgrade status of the managed devices.

Parameter	Description
copy list <mac-list>	Copy status of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.
reboot list <mac-list>	Reboot status of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.
summary list <mac-list>	Status summary of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.

Example

```
(host) [mynode] #show upgrade internal managed-devices status summary list
00:0b:23:b0:81:d0

upgrade managed-node status summary
-----
LC MAC   Config Path  Host Name  IP Addr  LC Model  Current Ver  Last Cmd
Last Cmd Status
-----
-----00:0b:23:b0:81:d0  /md/IND/70XXS  A7010-HA2-FIFTEEN
192.168.5.15  A7010  8.0.0.0-svcs-ctrl_55616  Not initialized  Not
initialized
```

The output of this command includes the following information:

Parameter	Description
LC MAC	MAC address of the managed device.
Config Path	Config node path of the managed device.
Host Name	Name of the Mobility Conductor.

Parameter	Description
IP Addr	IP address of the managed device.
LC Model	Model number of the managed device.
Current Ver	Version of ArubaOS currently running on the managed device.
Last Cmd	Last command issued on the managed device.
Last Cmd Status	Status of the last command issued on the managed device.

Related Commands

Command	Description
upgrade internal	This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device. This command is internal or hidden.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show upgrade managed-devices

```
show upgrade managed-devices status
  ca-bundle
    all
    path <node-path>
    single <mac-addr>
  copy
    all
    path <node-path>
    single <mac-addr>
  reboot
    all
    path <node-path>
    single <mac-addr>
  summary
    all
    path <node-path>
    single <mac-addr>
```

Description

This command displays the upgrade status of the managed devices.

Parameter	Description
ca-bundle	Trusted CA certificates version of managed device.
all	Trusted CA certificates version of all managed devices.
path <node-path>	Trusted CA certificates version of managed devices under the specific node path.
single <mac-addr>	Trusted CA certificates version of a managed device based on MAC address.
copy	Copy status of managed device.
all	Copy status of all managed devices under the respective node path.
path <node-path>	Copy status of all managed devices under the specific node path.
copy single <mac-addr>	Copy status of a specific managed device based on MAC address.
reboot	Reboot status of managed device.

Parameter	Description
all	Reboot status of all managed devices under the respective node path.
path	Reboot status of all managed devices under a specific node path.
single	Reboot status of a specific managed device based on MAC address.
Summary	Status summary of the managed device .
all	Status summary of all managed device under the respective node path.
path	Status summary ofl managed devices under a specific node path.
single	Status Summary of a specific managed device based on MAC address.

Example

```
(host) [mynode] #show upgrade managed-devices status summary single
00:0b:23:b0:81:d0
-----
LC MAC   Config Path  Host Name  IP Addr  LC Model  Current Ver  Last Cmd
Last Cmd Status
-----
00:0b:23:b0:81:d0  /md/IND/IPV6-NODES  A7005-BKLMS_TWENTY
2002:dead:face:5::20  A7005      8.0.0.0-svcs-ctrl_55616  Not initialized
Not initialized
```

The output of this command includes the following information:

Parameter	Description
LC MAC	MAC address of the managed device.
Config Path	Config node path of the managed device.
Host Name	Name of the Mobility Conductor.
IP Addr	IP address of the managed device.
LC Model	Model number of the managed device.

Parameter	Description
Current Ver	Version of ArubaOS currently running on the managed device.
Last Cmd	Last command issued on the managed device.
Last Cmd Status	Status of the last command issued on the managed device.

Related Commands

Command	Description
upgrade managed-devices	This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>ca-bundle</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show upgrade-profile

show upgrade-profile

Description

The settings in the centralized image upgrade profile uses ArubaOS images to upgrade the managed devices with the ArubaOS images hosted on an image server. When an upgrade action command is executed on the Mobility Conductor, the **upgrademgr** process running on Mobility Conductor sends an upgrade request to **upgrademgr** process running on corresponding managed devices. The managed devices then connect to the image server and download the appropriate image file after verifying the validity of the image file, before upgrading to the downloaded image file. The centralized image upgrade feature is enabled and configured on managed devices only, and supports up to 100 simultaneous image downloads.

Example

```
(host) (config) #show upgrade-profile

Upgrade Profile
-----
Parameter                Value
-----
Server IP address         N/A
Server IPv4/IPv6 address N/A
Username                  N/A
Password                  N/A
Protocol                  tftp
File path                  .
Download AOS Image from MM Enabled
```

The output of this command includes the following information:

Parameter	Description
serverip	The IPv4 address of the image server. This parameter is only used by managed devices running versions prior to ArubaOS 8.2 and accepts only IPv4 address. NOTE: For FTP or SCP protocol, specify the username and password.
serveraddr	The IPv4 or IPv6 address of the image server. This parameter is only used by managed devices running ArubaOS 8.2. NOTE: For FTP or SCP protocol, specify the username and

Parameter	Description
	password.
Username	If the <code>protocol</code> parameter is set to FTP or SCP , this parameter displays the user name that ArubaOS uses to connect to the image server.
Password	If the <code>protocol</code> parameter is set to FTP or SCP , this parameter displays the password that ArubaOS will use to connect to the image server.
Protocol	Specify the protocol used to send the software to the managed device. <ul style="list-style-type: none"> ▪ TFTP ▪ FTP ▪ SCP
File path	File path to the location on the image server where the image file(s) reside.
Download AOS Image from MM	If enabled, the flash storage on the Mobility Conductor is used as a file server for live upgrade and this locally stored image will be downloaded by the managed devices using HTTP protocol.

Related Commands

Command	Description
upgrade-profile	This command is used to configure the upgrade profile.

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>Download AOS Image from MM</code> parameter was added.
ArubaOS 8.2.0.0	The <code>serveraddr</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show uplink

```
show uplink
  cellular {config | connection-logs | details | mbn-profiles | signal}
  debug
  stats
  wired config
```

Description

Displays uplink manager configuration details.

Parameter	Description
cellular	Displays the cellular uplink configuration information.
config	Displays the passive cellular uplink configuration information.
connection-logs	Displays the cellular uplink connection logs.
details	Displays the internal cellular module details.
mbn-profiles	Displays the list of mobile broadband network profiles.
signal	Displays the cellular uplink signal information.
debug	Displays the uplink management debug information.
stats	Displays the statistical information on the designated uplink.
wired	Display the wired uplink information.
config	Displays the passive wired uplink configuration information.

Example

The output of this command displays the managed device uplink status . For a managed device, the health status of these uplink connections is also displayed in the **Status** section of the **Dashboard>WAN** page of the managed device WebUI.

```
(host) #show uplink

Uplink Manager: Disabled
Uplink Health-check: Disabled IP: 0.0.0.0
Uplink Management Table
-----
```

Uplink Type	Properties	Uplink-id	State	Gateway	Reachability	WAN Type
-----	-----	-----	-----	-----	-----	-----

Related Commands

Command	Description
ip probe default	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.
uplink	Manage and configure the uplink network connection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show usb

```
show usb
  cellular
  ports [<address>]
  test <address>
  usb-modeswitch
  verbose
```

Description

Display detailed USB device information on a stand-alone controller or managed device. This command should be executed from the managed device only.

Parameter	Description
cellular	Enter the keyword cellular to display cellular devices.
ports	Enter the keyword ports to display detailed TTY port information such as signal strength.
test	Enter the keyword test to test the USB TTY ports. NOTE: Testing an invalid modem port may cause the stand-alone controller or managed device to "hang". To resolve this, unplug and re-plug the modem.
usb-modeswitch	USB mode switch utility log.
verbose	Enter the keyword verbose to display detailed USB information including serial number and USB type.

Examples

The USB Device table, in the example below, displays the USB port is in the 'Device Ready' state, meaning that the port has passed the diagnostic test and is ready to send and receive data.

```
(host-md) #show usb

USB Device Table
-----
Address  Product      Vendor  ProdID  Serial          Type
Profile  State
-----  -
-----  -
18       Novatel Wireless CDMA  1410    4100    091087843891000 Cellular
new_modem Device ready
```

Below is an example of the `show usb verbose` display output (partial).

```
(host-md) #show usb verbose
...
T: Bus=01 Lev=02 Prnt=02 Port=00 Cnt=01 Dev#= 3 Spd=12 MxCh= 0
D: Ver= 1.10 Cls=00(>ifc ) Sub=00 Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=1410 ProdID=4100 Rev= 0.00
S: Manufacturer=Novatel Wireless Inc.
S: Product=Novatel Wireless CDMA
S: SerialNumber=091087843891000
C:* #Ifs= 5 Cfg#= 1 Atr=a0 MxPwr=500mA
...
```

Related Commands

Command	Description
usb	This command disconnects and reclassifies a USB device connected to a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show user

```
show user
  ap-group <ap-group>
  ap-name <ap-name>
  authentication-method dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web
  bssid <A:B:C:D:E:F>
  devtype <device>
  essid <STRING>
  internal
  ip <A.B.C.D> [log]
  location b.f.l
  mac <A:B:C:D:E:F> [log]
  mobile {[bindings][visitors]}
  name <STRING>
  phy-type {[a]|[b]}
  role <STRING>
  rows <NUMBER> <NUMBER>
```

Description

Displays detailed information about user in terms of AP group, authentication method, role and so on. Use the `show user` command to show detailed user statistics and roles.

Parameter	Description
ap-group <ap-group>	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
ap-name <ap-name>	Filter the output of this command by showing users connected to an AP with the specified AP name.
authentication-method	Filter the output of this command by the authentication method used for the device:
dot1x	Show data for devices using 802.1X authentication.
mac	Show data for devices using MAC authentication.
opensystem	Show data for devices using open (no) authentication.
psk	Show data for devices that do not use authentication but use a pre-shared key for encryption.
stateful-dot1x	Show data for devices using stateful 802.1X authentication.
via-vpn	Show data for devices that authenticate using Aruba VIA.
vpn	Show data for devices using VPN authentication.

Parameter	Description
web	Show data for devices using captive portal authentication.
bssid <A:B:C:D:E:F>	Show user data for a specific device BSSID.
devtype <device>	Show output for a specified device type, if identified. If the device name includes spaces, you must enclose it in quotation marks.
ssid <STRING>	Show user data for a specific ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Display internal user entries only. Include the rows options to filter the output of this command by specifying the number of rows from the end of the output and the total number of rows to display/
ip <A.B.C.D>	Show user data for a specific IP address .
log	If per-user logging is enabled using the aaa log command, include the optional <code>log</code> parameter to display authentication log files for a user with the specified MAC address.
mac <A:B:C:D:E:F>	Show user data for a specific MAC address
log	If per-user logging is enabled using the aaa log command, include the optional <code>log</code> parameter to display authentication log files for a user with the specified MAC address.
mobile	Filter the output of this command to show data for Mobile users.
bindings	Show data for users that have moved away from their home network.
visitors	Show data for mobility users that are visiting the network.
name <STRING>	User's name.
phy-type	801.11 type
a	Matches PHY type a.
g	Matches PHY type b or g.
role <STRING>	User role such as employee, visitor and so on.
rows <NUMBER> <NUMBER>	Filter the output of the show user command by specifying the number of rows from the end of the output and the total number of rows to display/

Example

```

(host) #show user
Users
-----
IP           MAC           Name   Role   Age(d:h:m)  Auth  VPN link  AP name
Roaming     Essid/Bssid/Phy  Profile Forward mode  Type  Host Name
-----
-----
User Entries: 0/0
Curr/Cum Alloc:0/0 Free:0/0 Dyn:0 AllocErr:0 FreeErr:0

```

Related Commands

Command	Description
user-role	This command configures a user role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show user-table

```
show user-table
  ap-group <ap-group>
  ap-name <ap-name>
  authentication-method dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web
  bssid <A:B:C:D:E:F>
  devtype <device>
  debug
  essid <STRING>
  internal
  ip <A.B.C.D> [log]|[detail]
  mac <A:B:C:D:E:F> [log]
  mobile {[bindings][visitors]}
  name <STRING>
  phy-type {[a]|[b]}
  role <STRING>
  rows <NUMBER> <NUMBER>
  standby [ipv4]|[ipv6]|[log]|[mac]
  station
  summary
  unique
  verbose
```

Description

Displays detailed information about the controller's connection to a user device, in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics. The `show user` command allows you to filter specific information by parameter. Use the `show user-table` command to show detailed user statistics which includes the entire output of the user-table, mobility state and statics, authentication statistics, VLAN assignment method, AP datapath tunnel information, radius accounting statistics, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics.

Parameter	Description
<code>ap-group <ap-group></code>	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
<code>ap-name <ap-name></code>	Filter the output of this command by showing users connected to an AP with the specified AP name.
<code>authentication-method</code>	Filter the output of this command by the authentication method used for the device:
<code>dot1x</code>	Show data for devices using 802.1X authentication.

Parameter	Description
mac	Show data for devices using MAC authentication.
opensystem	Show data for devices using open (no) authentication.
psk	Show data for devices that do not use authentication but use a pre-shared key for encryption.
stateful-dot1x	Show data for devices using stateful 802.1X authentication.
via-vpn	Show data for devices that authenticate using Aruba VIA.
vpn	Show data for devices using VPN authentication.
web	Show data for devices using captive portal authentication.
bssid <A:B:C:D:E:F>	Show user data for a specific device BSSID.
debug	Show all user data for debugging purposes.
devtype <device>	Show output for a specified device type, if identified. If the device name includes spaces, you must enclose it in quotation marks.
ssid <STRING>	Show user data for a specific SSID. If the SSID includes spaces, you must enclose it in quotation marks.
internal	Display internal user entries only. Include the rows options to filter the output of this command by specifying the number of rows from the end of the output and the total number of rows to display/
ip <A.B.C.D>	Show user data for a specific IP address .
log	If per-user logging is enabled using the aaa log command, include the optional <code>log</code> parameter to display authentication log files for a user with the specified MAC address.
detail	Show detailed user data for a specific IP address including role-derivation.
mac <A:B:C:D:E:F>	Show user data for a specific MAC address
log	If per-user logging is enabled using the aaa log command, include the optional <code>log</code> parameter to display authentication log files for a user with the specified MAC address.
mobile	Filter the output of this command to show data for Mobile users.
bindings	Show data for users that have moved away from their home network.

Parameter	Description
visitors	Show data for mobility users that are visiting the network.
name <STRING>	User's name.
phy-type	801.11 type
a	Matches PHY type a.
g	Matches PHY type b or g.
role <STRING>	User role such as employee, visitor and so on.
rows <NUMBER> <NUMBER>	Filter the output of the show user command by specifying the number of rows from the end of the output and the total number of rows to display/
standby	User standby entries
ipv4	User standby entries for the IPv4 address specified.
ipv6	User standby entries for the IPv6 address specified.
log	Debug log of the specified user.
mac	User standby entires for the MAC address specified.
station	For internal use only.
summary	Shows the authentication and encryption type used by wired or wireless clients.
unique	Displays only information for users with a valid IP address.
verbose	Displays all information about the user table.

Examples

This example displays users currently in the **employee** role. The output of this command is split into two tables in this document, however it appears in one table in the CLI.

```
(host) [mynode] (config) show user-table role employee
Users
-----
      IP                MAC                Name                Role                Age (d:h:m)
Auth   VPN link   AP name
-----
-----
192.168.160.1  00:23:6c:80:3d:bc  madison1            employee            01:05:50
802.1X                1263
```

```

10.100.105.100 00:05:4e:45:5e:c8 CORP1NETWORKS employee 00:02:22
802.1X wlan-qa-cage
10.100.105.102 00:14:a5:30:c2:7f pdedhia employee 01:20:09
802.1X 2198
10.100.105.97 00:1b:77:c4:a2:fa CORP1NETWORKS employee 00:02:18
802.1X 2198
10.100.105.109 00:21:5c:02:16:bb myao employee 00:05:40
802.1X 1109

```

Users

Roaming Type	Essid/Bssid/Phy	Profile	Forward mode
-----	-----	-----	-----
Associated	ethersphere-wpa2/00:1a:1e:85:d3:b1/a-HT	default	tunnel
Associated	ethersphere-wpa2/00:1a:1e:6f:e5:51/a	default	tunnel
Associated	ethersphere-wpa2/00:1a:1e:87:ef:f1/a	default	tunnel
Associated	ethersphere-wpa2/00:1a:1e:87:ef:f1/a	default	tunnel
Associated	ethersphere-wpa2/00:1a:1e:85:c2:11/a-HT	default	tunnel

ipad

The output of the `show user mac <mac-addr>` and `show user ip <ip-addr>` commands include the following information.

```

(host) [mynode]) # show user-table ip 5.5.5.2
Name: 98:0c:82:45:d6:7b, IP: 5.5.5.2, MAC: 98:0c:82:45:d6:7b, Role: mac-
role, ACL: 54/0/0, Age: 00:00:07
Authentication: Yes, status: started, method: MAC, protocol: PAP, server:
Internal
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: default for authentication type MAC
VLAN Derivation: unknown
Idle timeouts: 0, Valid ARP: 0
Mobility state: Wireless, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0
L3 Mob: 0
Flags: internal=0, trusted_ap=0, l3auth=0, mba=1, vpnflags=0, u_stm_ageout=1
Flags: innerip=0, outerip=0, vpn_outer_ind:0, guest=0, download=1, wispr=0
Auth fails: 0, phy_type: g-HT, reauth: 0, BW Contract: up:0 down:0, user-
how: 14
Vlan default: 3, Assigned: 5, Current: 5 vlan-how: 0 DP assigned vlan:0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, Flags=0x0
Tunnel=0, SlotPort=0x2000, Port=0x1000d (tunnel 13)
Role assignment - L3 assigned role: n/a, VPN role: n/a, Dot1x cached role:
n/a
Current Role name: mac-role, role-how: 1, L2-role: mac-role, L3-role: mac-
role
Essid: 1_wlan_135, Bssid: d8:c7:c8:38:f4:a0 AP name/group:
d8:c7:c8:cb:8f:4a-135/groupfor135 Phy-type: g-HT
RadAcct sessionID:n/a
RadAcct Traffic In 4/216 Out 2/420 (0:4/0:0:0:216,0:2/0:0:0:420)
Timers: reauth 0
Profiles AAA:1_wlan_135-aaa_prof, dot1x:dot1x_prof-rwv10, mac:pMac CP: def-
role:'logon' sip-role:'' via-auth-profile:''

```

```

ncfg flags udr 0, mac 1, dot1x 1, RADIUS interim accounting 0
IP Born: 1354560806 (Mon Dec 3 10:53:26 2012)
Core User Born: 1354560805 (Mon Dec 3 10:53:25 2012)
Upstream AP ID: 0, Downstream AP ID: 0
Device Type: Dalvik/1.4.0 (Linux; U; Android 2.3.6; SAMSUNG-SGH-I777
Build/GINGERBREAD)
Session Timeout from Radius: No, Session Timeout Value:0
Address is from DHCP: yes

```

The `role-how` and `vlan-how` parameters in the output of this command display a code that corresponds to the following values:

Role Derivation Code	Description
1	AAA profile default role
2	Role derived from user rules
3	Role derived from UDR
4	Default role for authentication type
5	Role derived from server rules
6	Aruba vendor-specific attribute (VSA)
7	Dot1X profile role
8	Dot1X server derived role
9	Dot1X role derived from Aruba VSA
10	Dot1X role derived from ClearPass Policy Manager VSA
11	Role derived from DHCP option
12	Change of authorization role
13	Forced role set by ESI
14	Role derived from mobility
15	Role assigned by external/internal captive portal
16	Role assigned by SIP
17	SDR derived role during L3 authentication
18	VSA derived role during L3 authentication

Role Derivation Code	Description
19	ClearPass Policy Manager VSA derived role during L3 authentication
20	Authentication type VPN role (VIA, VPN, or Transport VPN)
21	Authentication type role (BTLM, Kerb, GIS, or so on)
22	System assigned AP role

VLAN Derivation Code	Description
1	Default VLAN
2	Initial role contained
3	User rule role contained
4	Matched user rule
5	DHCP Option 77 role contained
6	Matched DHCP Option 77
7	MBA role contained
8	MBA server rule role contained
9	MBA server rule
10	MBA Aruba VSA role contained
11	MBA Aruba VSA
12	MBA MSFT attributes
13	User Dot1X role contained
14	Dot1X server rule role contained
15	Dot1X server rule
16	Dot1X Aruba VSA role contained
17	Dot1X Aruba VSA
18	Dot1X MSFT attributes
19	VLAN from pmk-cache

VLAN Derivation Code	Description
20	DHCP options user rule role contained
21	DHCP options user rule
30	Adaptive DHCP VLAN

Related Commands

Command	Description
user-role	This command configures a user role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show util_proc

```
show util_proc guest-email counters
```

Description

Show counters for the guest email process. As part of guest provisioning, the guest access email feature allows you to define the SMTP port and server that processes guest provisioning email. This server sends email to the guest or the sponsor when a guest user manually sends email from the Guest Provisioning page, or when a user creates a guest account.

Example

The output of this command shows the numbers of guest emails received, sent and dropped since the controller was last reset

```
(host) #show util_proc guest-email counters

Guest Email Counters
-----
Name                Value
----                -
Email Received      14
Email Sent           3
Email Dropped       0.
```

Related Commands

Command	Description
guest-access-email	This command configures SMTP servers and server ports for guest email.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show valid-network-oui-profile

show valid-network-oui-profile

Description

This command displays the Valid Equipment OUI Profile table. If you use the valid-networkoui-profile to add a new OUI to the controller, use the show valid-network-oui-profile command to see a list of current OUIs.

Example

```
(Host) (config) #show valid-network-oui-profile

Valid Equipment OUI profile
-----
Parameter  Value
-----
OUI         00:1A:1E
```

Related Commands

Command	Description
valid-network-oui-profile	This command allows you to add a new OUI to the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show version

```
show version
```

Description

Shows the system software version.

Example

```
(host) #show version
Aruba Operating System Software.
      ArubaOS (MODEL: Dell Networking W-650 Controller-US),
Version 6.1.0.0
Website: http://www.dell.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-04-28 at 00:18:36 PDT (build 28106) by p4build

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 23274)
Built: 2010-01-19 11:11:41
Built by: p4build@re_client_23274

Switch uptime is 1 days 6 hours 2 minutes 4 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 408 (revision B1) with 890M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

The output of this command includes the following information

Parameter	Description
Model	controller model type.
Version	Version of ArubaOS software.
ROM	System bootstrap version.
Switch Uptime	Switch uptime (time elapsed since the last controller reset.
Reboot Cause	Reason the controller was last rebooted.
Supervisor Card	Details for the controller's internal supervisor card.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show via

```
show via
  version
  websessions
  lastlogin
```

Description

Displays the VIA version and web session details.

Parameter	Description
version	Displays the version of VIA client available on the controller.
websessions	Displays the list of users connected to the VIA controller using the VIA client.
lastlogin	Displays the time that the VIA user last logged in.

Example

The following example displays the version of VIA client available on the controller.

```
(host) # show via version(host) (VIA Client WLAN Profile "example") #show
via version
Default VIA Installer:
-----
<aruba>
  <via>
    <platform>win32</platform>
    <version>1.0.0.23373</version>
  </via>
</aruba>
The following example displays the time that the VIA user last logged in.
(host) [mm] #show via-lastlogin
VIA users login Details
-----
User Name   Last Login Time (GMT)
-----
vpatil123  Wed Jun 20 16:41:19 2018
abc123     Fri Jun 22 05:40:48 2018
smidha     Fri Jun 22 06:55:59 2018
vpatil     Fri Jun 22 09:30:13 2018
Total Entries: 4
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>lastlogin</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vlan

```
show vlan
  mapping
  status
  summary
  <id>
```

Description

This command shows VLAN settings. Click parameter links to view the corresponding show commands.

Parameter	Description
mapping	Show vlan name mapping.
status	Show vlan status.
summary	VLAN summary information.
vlan <id>	VLAN Interface number. 1-4094 1

Example

```
(hots) #show vlan
VLAN CONFIGURATION
-----
VLAN  Description  Ports                AAA Profile  Option-82
----  -
1      Default         GE0/0/0-0/1 Pc0-7  N/A         Disabled
102    VLAN0102        GE0/0/0             N/A         Disabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vlan mapping

show vlan mapping

Description

This command shows a configured VLAN name, its pool status, assignment type, and the VLAN IDs assigned to the pool. Use this command to show the selected VLAN configuration. The **VLAN Name** column displays the name of the VLAN pool. The **VLAN IDs** column lists the VLANs that are part of the pool.

Parameter	Description
<id>	Identification number for the VLAN. 1-4094 1

Example

```
(Host) [mynode] (config) #show vlan mapping
Vlan Mapping Table
-----
VLAN Name  Assignment Type  VLAN IDs      IP Timeout  Max IP Timeouts Full
Period
-----
-----
-----
-----
-----
a          Even             1001-1002     10          3
30
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters IP Timeout, Max IP Timeouts and Full Period were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show vlan status

```
show vlan status <id>
```

Description

This command shows the current status of all VLANs on the controller. Use this command to show the status of VLANs on the controller. The **VLAN ID** column displays the VLAN ID name or number. The **IP Address** column provides the VLAN's IP address. The **Adminstate** column indicates if the VLAN is enabled or disabled. The **Operstate** column indicates if the VLAN is currently up and running. The **PortCount** column shows how many ports are associated with the VLAN. The **Nat Inside** column displays whether source Nat is enabled for the VLAN interface. If Nat is enabled, all the traffic passing through this VLAN interface is the source natted to the outgoing interface's IP address.

Example

```
(host) #show vlan status

Vlan Status
-----
VlanId  IPAddress                               Adminstate  Operstate  PortCount  Nat
Inside  Mode    Ports                               -----  -----  -----  -----
-----  -----  -----
1        unassigned/unassigned                 Enabled     Up          9
Disabled Regular GE1/0 GE1/2 GE1/5-9 XG1/10-11 Pc0 Pc2-5 Pc7  N/A
2        N/A                                     N/A        N/A        3
Disabled Regular GE1/7-9
10       172.20.10.202/255.255.255.0           Enabled     Up          4
Disabled Regular GE1/7-9 Pc6
21       172.20.21.202/255.255.255.0           Disabled    Down        4
Disabled Regular GE1/7-9
24       172.20.24.202/255.255.255.0           Disabled    Down        3
Disabled Regular GE1/7-9
29       172.20.29.202/255.255.255.0           Enabled     Up          4
Disabled Regular GE1/7-9 Pc6
101      172.102.1.202/255.255.255.0           Enabled     Down        3
Disabled Regular GE1/7-9
102      172.102.2.202/255.255.255.0           Enabled     Down        3
Disabled Regular GE1/7-9
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show vlan summary

show vlan summary

Description

This command shows the number of existing VLANs. Use this command to show the number of existing VLANs on the controller.

Parameter	Description
Number of existing VLANs	The number of existing VLANs on the controller.

Example

```
(host) #show vlan summary
Number of existing VLANs      :13
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show vlan id

show vlan <id>

Description

This command shows a configured VLAN interface number, description and associated ports. Issue this command to show the selected VLAN configuration. The **VLAN** column lists the VLAN ID. The **Description** column provides the VLAN name or number and the **Ports** column shows the VLAN's associated ports. The **AAA Profile column** shows if a wired AAA profile has been assigned to a VLAN, enabling role-based access for wired clients connected to an untrusted VLAN or port on the controller.

Parameter	Description
<id>	Identification number for the VLAN. 1-4094 1

```
(host) #show vlan 102
VLAN CONFIGURATION
-----
VLAN  Description  Ports      AAA Profile  Option-82
----  -
102   VLAN0102    GE0/0/0    N/A          Disabled
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vlan-assignment

```
show vlan-assignment
```

Description

This command shows the number of clients assigned to a VLAN. Issue this command to show the number of clients that are assigned to a VLAN.

```
(host) [mynode]#show vlan-assignment

VLAN Assignment
-----
VLAN  #CLIENTS  IP TIMEOUT COUNT  TIME FULL
-----
1001   1           3                 39
1002   1           0                 0
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.7.0.0	The output parameters IP Timeout Count and Time Full were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vlan-assignment-auth

show vlan-assignment-auth

Description

This command shows the VLAN usage in the user authentication module. Issue this command to view all the VLAN IDs that are configured along with the current client count that uses that VLAN ID.

```
(host) #show vlan-assignment-auth

Vlan usage in AUTH
-----
VLAN ID  Usage
-----
10       0
```

Related Commands

Command	Description
vlan	This command creates a VLAN ID or a range of VLAN IDs on the managed device.
vlan-name	This command creates a named VLAN on the managed device and given an assignment type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vlan-bwcontract-explist

show vlan-bwcontract-explist [internal]

Description

Show entries in the VLAN bandwidth contracts MAC exception lists.

Parameter	Description
internal	Include the optional <code>internal</code> parameter to display the MAC addresses in the internal, preconfigured VLAN bandwidth contracts MAC exception list.

Example

The following command displays the MAC addresses in the internal MAC exception list.

```
(host) (config) #show vlan-bwcontract-explist internal

VLAN BW Contracts Internal MAC Exception List
-----
MAC address
-----
01:80:C2:00:00:00
01:00:0C:CC:CC:CD
01:80:C2:00:00:02
01:00:5E:00:82:11
```

Related Commands

Command	Description
vlan-bwcontract-explist	This command is used to add entries to or remove entries from the MAC exception list for bandwidth contracts on broadcast or multicast traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show vpdn

```
show vpdn
  l2tp
  pptp
  tunnel
```

Description

This command shows the vpdn configuration settings. Click parameter links to view the corresponding show commands.

Parameter	Description
l2tp	Show vpdn L2TP state.
pptp	Show pptp state.
tunnel	Show vpdn tunnel state.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show vpdn l2tp

```
show vpdn l2tp
  configuration
  local pool <pool_name>
```

Description

Displays the VPN L2TP state.

Parameter	Description
configuration	Show L2TP configuration.
local pool <pool_name>	Show l2tp local IP pool.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn l2tp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.16.15.1
DNS secondary server: 10.16.14.1
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
  PAP
IP LOCAL POOLS:
  vpnpool: 10.16.15.150 - 10.16.15.160
```

Related Commands

Command	Description
vpdn group l2tp	This command configures an L2TP or IPsec VPN connection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show vpdn tunnel

show vpdn tunnel <l2tp>

Description

Displays the VPN L2TP tunnel state.

Example

The output of this command shows the L2TP tunnel state.

```
(host) #show vpdn tunnel l2tp
% No active L2TP Tunnel
L2TP Statistics:
IPSEC Deletes: 0
IPSEC Sync-Deletes: 0
Hello Timeouts: 0
```

Related Commands

Command	Description
show vpdn l2tp configuration	Displays the VPN L2TP tunnel configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show vpdn pptp

```
show vpdn pptp
  configuration
  local
```

Description

This command shows the vpdn pptp settings. Click parameter links to view the corresponding show commands.

Parameter	Description
configuration	Show PPTP configuration.
local	Show pptp local IP pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show vpdn pptp configuration

show vpdn pptp configuration

Description

Displays the PPTP configuration on the controller.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn pptp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.15.1.1
DNS secondary server: 10.15.1.200
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
    MSCHAP
    MSCHAPv2
MPPE Configuration
    128 bit encryption enabled
IP LOCAL POOLS
```

Related Commands

Command	Description
vpdn group pptp	This command configures a PPTP VPN connection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show vpdn pptp local pool

```
show vpdn pptp local pool <pool_name>
```

Description

Displays the IP address pool for VPN users using Point-to-Point Tunneling Protocol.

Example

The output of this command shows the all IP address pools for VPN users.

```
(host) # show vpdn pptp local pool
IP addresses used in pool localgroup
0 IPs used - 11 IPs free - 11 IPs configured
```

Related Commands

Command	Description
vpdn group pptp	This command configures a PPTP VPN connection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show vpn-dialer

```
show vpn-dialer <dialer_name>
```

Description

Displays the VPN dialer configuration for users using VPN dialers.

Example

The output of this command shows the VPN dialer configuration for remote users.

```
(host) # show vpn-dialer remoteUser

remoteUser
-----
Attribute          Value
-----
PPTP                disabled
L2TP                enabled
DNETCLEAR          disabled
WIREDNOWIFI        disabled
PAP                enabled
CHAP               enabled
MSCHAP             enabled
MSCHAPV2           enabled
CACHE-SECURID     disabled
IKESECS            4000
IKEENC             3DES
IKEGROUP           ONE
IKEHASH            MD5
IKEAUTH            PRE-SHARE
IKEPASSWD          *****
IPSECSECS          4000
IPSECGROUP         GROUP1
IPSECENC           ESP-3DES
IPSECAUTH          ESP-MD5-HMAC
SECURID_NEWPINMODE disabled
```

Related Commands

Command	Description
vpn-dialer	This command configures the VPN dialer.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor and managed devices.

show vrrp

```
show vrrp {{<vrid>[statistics]}|ipv6<vrid>|stats[all]}|stats[all]|summary}
```

Description

Displays the list of all VRRP configuration on the managed device. To view a specific VRRP configuration, specify the VRID number.

Parameter	Description
<vrid>	Displays the Virtual Router Id. 1-255
ipv6	Display VRRP information for IPv6 address.
stats	Displays the operational statistics of the VRRP.
summary	Displays the number of vrrp instances for IPv4 and IPv6.

Example

The output of the following command shows the VRRP IPv4 instance with vrid 1.

```
(host) [mynode] #show vrrp
Virtual Router 1:
Description
Admin State UP, VR State BACKUP
IP Address 0.0.0.0, MAC Address 00:00:5e:00:01:01, vlan 99
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
Hold time 45 sec
Auth type NONE *****
tracking is not enabled
```

The output of the following command shows the statistics for IPv4 vrrp instance with vrid 10.

```
(host) [mynode] # show vrrp 10 statistics
Virtual Router 10:
Admin State UP, VR State MASTER
Advertisements:
Sent:                249562   Received:                475
Zero priority sent:      0   Zero priority received:  0
Lower IP address received 475   Lower Priority received  3
Tracking priority overflow: 0
Advertisements received errors:
Interval mismatch      0   Invalid TTL              0
Invalid packet type    0   Authentication failure   0
```

```

Invalid auth type          0   Mismatch auth type          0
Invalid VRRP IP address   0   Invalid packet length       0
VRRP Up timestamp:       Fri Aug 23 15:49:27 2013
Master Up timestamp:     Mon Aug 26 11:59:44 2013
Last advertisement sent timestamp: Mon Aug 26 16:38:55 2013
Last advertisement received timestamp: Mon Aug 26 11:59:44 2013
Current time:           Mon Aug 26 16:38:55 2013
Number times became VRRP Master: 2

```

The output of the following command provides information about IPv6 VRRP instances.

```

(host) [mynode] # show vrrp ipv6
Virtual Router 1:
Description
Admin State DOWN, VR State INIT
IPv6 Address ::
MAC Address 00:00:5e:00:02:01, vlan 0
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled
Virtual Router 23:
Description
Admin State DOWN, VR State INIT
IPv6 Address ::
MAC Address 00:00:5e:00:02:17, vlan 0
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled
Virtual Router 255:
Description
Admin State UP, VR State MASTER
IPv6 Address 2006::25
MAC Address 00:00:5e:00:02:ff, vlan 521
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled

```

The output of the following command shows the statistics for IPv6 VRRP instances.

```

(host) [mynode] #show vrrp ipv6 stats all
Virtual Router 1:
Admin State DOWN, VR State INIT
Advertisements:
Sent:          0   Received:
  0
Zero priority sent: 0   Zero priority received:
  0
Lower IP address received 0   Lower Priority received
  0
Tracking priority overflow: 0
Advertisements received errors:
Interval mismatch 0   Invalid TTL
  0
Invalid packet type 0

```

```

Invalid VRRP IP address          0   Invalid packet length
0
VRRP Up timestamp:              N/A, DOWN
Master Up timestamp:            N/A, not MASTER
Last advertisement sent timestamp: never
Last advertisement received timestamp: never
Current time:                   Wed Sep 25 19:40:42 2013
Number times became VRRP Master: 0
Virtual Router 23:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                            0   Received:
0
Zero priority sent:              0   Zero priority received:
0
Lower IP address received        0   Lower Priority received
0
Tracking priority overflow:      0
Advertisements received errors:
Interval mismatch                0   Invalid TTL
0
Invalid packet type              0
Invalid VRRP IP address          0   Invalid packet length
0
VRRP Up timestamp:              N/A, DOWN
Master Up timestamp:            N/A, not MASTER
Last advertisement sent timestamp: never
Last advertisement received timestamp: never
Current time:                   Wed Sep 25 19:40:42 2013
Number times became VRRP Master: 0

```

The output of the following command shows VRRP IPv4 and IPv6 instances.

```

(host) [mynode] #show vrrp summary
Number of existng VRRP IPv4 instances :    2
Number of existng VRRP IPv6 instances :    3

```

The output of the following command shows the configuration for all IPv6 VRRP instances.

```

(host) [mynode] #show vrrp ipv6
Virtual Router 1:
Description
Admin State DOWN, VR State INIT
IPv6 Address ::
MAC Address 00:00:5e:00:02:01, vlan 0
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled
Virtual Router 23:
Description
Admin State DOWN, VR State INIT
IPv6 Address ::
MAC Address 00:00:5e:00:02:17, vlan 0

```

```

Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled
Virtual Router 255:
Description
Admin State UP, VR State MASTER
IPv6 Address 2006::25
MAC Address 00:00:5e:00:02:ff, vlan 521
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
tracking is not enabled

```

The output of the following command shows the statistics for IPv4 VRRP instances.

```

(host) [mynode] #show vrrp stats all
Virtual Router 1:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                0   Received:                                0
Zero priority sent:                  0   Zero priority received:                  0
Lower IP address received            0   Lower Priority received                  0
Tracking priority overflow:          0
Advertisements received errors:
Interval mismatch                    0   Invalid TTL                             0
Invalid packet type                  0   Authentication failure                   0
Invalid auth type                    0   Mismatch auth type                      0
Invalid VRRP IP address              0   Invalid packet length                   0
VRRP Up timestamp:                  N/A, DOWN
Master Up timestamp:                 N/A, not MASTER
Last advertisement sent timestamp:    never
Last advertisement received timestamp: never
Current time:                        Wed Sep 25 19:55:33 2013
Number times became VRRP Master:     0
Virtual Router 23:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                0   Received:                                0
Zero priority sent:                  0   Zero priority received:                  0
Lower IP address received            0   Lower Priority received                  0
Tracking priority overflow:          0
Advertisements received errors:
Interval mismatch                    0   Invalid TTL                             0
Invalid packet type                  0   Authentication failure                   0
Invalid auth type                    0   Mismatch auth type                      0
Invalid VRRP IP address              0   Invalid packet length                   0
VRRP Up timestamp:                  N/A, DOWN
Master Up timestamp:                 N/A, not MASTER
Last advertisement sent timestamp:    never
Last advertisement received timestamp: never
Current time:                        Wed Sep 25 19:55:33 2013
Number times became VRRP Master:     0

```

Related Commands

Command	Description
vrrp	This command configures the VRRP.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Conductor.

show web-cc

```
show web-cc
  categories
  reputation
  md
    stats
  mm
    stats
  stats
  status
  global-bandwidth-contract all|{web-cc-category <category>}|{web-cc-reputation
<reputation>}
```

Description

Displays information about web content (web-cc) classification settings, category and reputation types, classification statistics and bandwidth contracts. The web content classification feature classifies all (HTTP/HTTPS) web traffic on the network. The output of the `show web-cc` command displays information about Webroot classification categories and risk reputation levels, bandwidth contracts, and the web content classification cache and database.

Parameter	Description
categories	Display the category index number and the category name for each category type.
md stats	Display web content classification table statistics for the managed device. This command must be issued on the managed device.
mm stats	Display web content classification table statistics for Mobility Conductor.
reputation	Display the different reputation levels, and the range of reputation scores associated with each level.
stats	Display counters for web content traffic and web content classification table statistics
status	Display information about the current operational status of the web content classification feature.
global-bandwidth-contract	Display settings for global bandwidth contracts assigned to web content classification category types and reputation levels.
all	Show all bandwidth contracts

Parameter	Description
web-cc-category <category>	Display information for the specified web-cc category bandwidth contract.
web-cc-reputation <reputation>	Display information for the specified web-cc reputation bandwidth contract.

Examples

To see if the WebCC feature is able to send queries from Mobility Conductor to the WebRoot server in the cloud, issue the command `show web-cc status`.

```
(host)[mynode](config) #show web-cc status
Web Content Classification Status
-----
Service Status
-----
Web Content Classification enabled :    Yes
DNS/Name Server configured :          Yes
URL Cloud lookup server reachable :    Yes
Cloud lookup/update available :        Yes
Webroot Server Connection Type :      ipv6
Mode:                                  MM
```

The following command shows the global bandwidth contracts applied to upstream and downstream traffic matching the **music** content category.

```
(host)[mynode](config) #show web-cc global-bandwidth-contract web-cc-
category music
Web-cc Global Bandwidth Contract
-----
Web-cc Category/Reputation  Direction  Rate (bits/second)  Contract  Id
-----
web-cc-category music      Upstream    55000000            music-2126  2
web-cc-category music      Downstream  20000000            music-745c  1
```

The output of the `show web-cc` command varies, depending upon the parameters specified. The following table describes the information displayed in the output of this command when that parameter is included.

Parameter	Description
categories	Include this parameter to display the following information categories in the command output: <ul style="list-style-type: none"> ▪ Name: names of the available web content classification categories

Parameter	Description
	<ul style="list-style-type: none"> ▪ Web Category ID: ID number associated with a category name
reputation	<p>Include this parameter to display the following information categories in the command output:</p> <ul style="list-style-type: none"> ▪ RiskLevel: names of the available web content classification risk levels ▪ Score: Range of risk scores associated with a risk level
Stats	<p>Include this parameter to display the following information categories in the command output:</p> <ul style="list-style-type: none"> ▪ URL miss from sos: number of times a URL was not found in the internal web content classification cache. ▪ Database hit: number of times a URL was not found in the internal web content classification cache, but was found by the local web content classification database. ▪ Cloud lookup: number of times a URL was not found by the local web content classification database, and was sent to the cloud for identification. ▪ Cloud response: number of times the cloud responded to a cloud lookup request. ▪ RTU updates: Number of times that the internal web content classification cache was updated ▪ DB Entries: Maximum number of entries allowed in the local web content classification database. This value varies by controller type.
Status	<p>Include this parameter to display the following information categories in the command output:</p> <ul style="list-style-type: none"> ▪ Web Content Classification enabled: Displays if the web content classification feature is enabled or disabled. ▪ DNS/Name Server configured: Displays if DNS is configured on the controller. The web content classification feature uses DNS to identify the URL cloud server, so DNS must be configured on the controller for this feature to work. ▪ Cloud lookup/update available: A status of Yes indicates that license pool for that configuration node has a sufficient number of unexpired Web Content Classification licenses. A status of No indicates that licenses have expired, or that there are not enough licenses for the managed devices in that pool. ▪ URL Cloud lookup server reachable: Indicates if the controller is able to contact the URL cloud server.

Parameter	Description
	<ul style="list-style-type: none"> ▪ Webroot Server Connection Type: Displays if the connection to the Webroot server to look-up or download the URL database is by using IPv4 or IPv6 addresses. ▪ Mode: Indicates operational mode for the WebCC feature. If the managed device is in centralized mode, the Mobility Conductor (MM) contacts the WebRoot server for URL queries. If the managed device is in distributed mode, the managed device contacts the WebRoot server directly.
global-bandwidth-contract	<p>Include this parameter to display the following information categories in the command output:</p> <ul style="list-style-type: none"> ▪ Web-cc Category/Reputation: Name of the web content classification category or reputation level. ▪ Direction: indicates whether the contract applies to upstream or downstream traffic. ▪ Rate (bits/second) : bandwidth contract rate, in bits/second. ▪ Contract: unique name assigned to the web-cc global bandwidth contract. ▪ Id: identification number assigned to the web-cc global bandwidth contract.

The following output displays the current operational status of web content classification feature when the managed device is in the default centralized WebCC mode or in distributed mode:

```

MD : Webcc mode: Centralized
-----
(Aruba7210) #show web-cc status

Web Content Classification Status
-----
Service                               Status
-----
Web Content Classification enabled :   Yes
DNS/Name Server configured :          Yes
URL Cloud lookup server reachable :    Yes
Cloud lookup/update available :       Yes
Webroot Server Connection Type :      ipv6
Mode :                                 MD - Centralized
MM IP address :                        10.15.60.251

MD : Webcc mode: Distributed
-----
(Aruba7210) #show web-cc status

Web Content Classification Status

```

```

-----
Service                               Status
-----
Web Content Classification enabled :   Yes
DNS/Name Server configured :          Yes
URL Cloud lookup server reachable :    Yes
Cloud lookup/update available :        Yes
Webroot Server Connection Type :      ipv6
Mode :                                 MD - Distributed
MM IP address :                        10.15.60.251

```

Related Commands

Command	Description
web-cc global-bandwidth-contract	This command defines global bandwidth contracts for HTTP traffic matching a predefined web content category or reputation type.

Command History

Release	Modification
ArubaOS 8.4.0.0	The Webroot Server Connection Type field was added to the output of the <code>show webcc-status</code> command.
ArubaOS 8.2.0.0	The Mode and Cloud lookup/update available fields were added to the output of the <code>show webcc-status</code> command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	WebCC license	Enable and Config mode on Mobility Conductor.

show web-proxy

show web-proxy

Description

Displays information about the port and server configured for the web-proxy.

Example

The following command shows the port configured for the web-proxy server.

```
(host) [mynode] #show web-proxy
Server: exampleproxy.com
port: 8080
```

Related Commands

Command	Description
web-proxy server	This command configures the web-proxy server related information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show web-server

```
show web-server
  profile
  statistics
```

Description

Displays the configuration and statistics of the controller web server.

Parameter	Description
profile	Displays the web server configuration profile.
statistics	Displays the web server statistics. This command helps to troubleshoot Captive Portal scale issues.

Example

The output of this command shows the web-server configuration.

```
(host) [mynode]# show web-server profile

Web Server Configuration
-----
Parameter                               Value
Set
-----
-
Cipher Suite Strength                    high
SSL/TLS Protocol Config                  tlsv1.2
Switch Certificate                        default-self-signed
Captive Portal Certificate               default
IDP Certificate                          default-self-signed
Management user's WebUI access method   username/password
User absolute session timeout <30-3600> (seconds) 0
User session timeout <30-3600> (seconds) 900
Maximum supported concurrent clients <25-320> 25
Enable WebUI access on HTTPS port (443)  false
Enable bypass captive portal landing page  false
Exclude Security Headers from HTTP Response false
```

Starting from 8.11.0.0, the output of this command displays the list of selected cipher suites configured for the web server profile.

```
(host) [mynode]# show web-server profile

Web Server Configuration
```



```

-----
Parameter                               Value
Set                                     -----
-----
-
Enable provided cipher suites            ECDHE-ECDSA-AES256-GCM-
SHA384 ECDHE-ECDSA-AES128-GCM-SHA256  ECDHE-RSA-AES256-GCM-SHA384
                                         ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES2
ECDSA-AES128-SHA256
                                         ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SH
                                         ECDHE-RSA-AES128-SHA
SSL/TLS Protocol Config                 tlsv1.2
Switch Certificate                       default
Captive Portal Certificate              default
IDP Certificate                         default
Management user's WebUI access method  username/password
User absolute session timeout <30-3600> (seconds) 0
User session timeout <30-3600> (seconds) 900
Maximum supported concurrent clients <25-320> 75
Enable WebUI access on HTTPS port (443) false
Enable bypass captive portal landing page false
Exclude Security Headers from HTTP Response false
VIA client-cert port number            8085

```

The output of this command displays the web-server statistics.

```

(host) #show web-server statistics

Web Server Statistics:
-----
Current Request Rate:          1 Req/Sec
Current Traffic Rate:          0 KB/Sec
Busy Connection Slots:         1
Available Connection Slots:    24
Total Requests Since Up Time:  16854
Total Traffic Since Up Time:   199580 KB
Avg. Request Rate Since Up Time: 0 Req/Sec
Avg. Traffic Rate Since Up Time: 321 Bytes/Sec
Server Scoreboard _____W_____

Scoreboard Key: _ - Waiting for Connection, s - Starting up
                R - Reading Request, W - Sending Reply
                K - Keepalive, D - DNS Lookup
                C - Closing connection, L - Logging
                G - Gracefully finishing, I - Idle cleanup of worker
                . - Open slot with no current process

```

The output of the `show web-server statistics` command includes the following parameters.

Parameter	Description
Current Request Rate	HTTP/HTTPS request rate measured immediately within the last one second.
Current Traffic Rate	HTTP/HTTPS data transfer rate measured immediately within the last one second.
Busy Connection Slots	Number of simultaneous HTTP/HTTPS sessions currently being served. Each session occupy one slot from the total available slot configured under the web-max-clients < web-max-client > parameter.
Available Connection Slots	Number of simultaneous HTTP/HTTPS sessions which can be served more than what is being served currently.
Total Requests Since Up Time	Total number of HTTP/HTTPS requests received by the web server since the server was up.
Total Traffic Since Up Time	Total number of HTTP/HTTPS traffic handled by the web server since the server was up.
Avg. Request Rate Since Up Time	Lifetime average of HTTP/HTTPS request rate. This is calculated by dividing the total number of requests received with the web server up-time.
Avg. Traffic Rate Since Up Time	Lifetime average of HTTP/HTTPS traffic rate. This is calculated by dividing the total of HTTP/HTTPS traffic with the web server up-time.
Server Scoreboard	Displays information of each worker thread of web server.

Related Commands

Command	Description
web-server profile	This command configures the Mobility Conductor's web server.

Command History

Release	Modification
ArubaOS 8.11.0.0	The Cipher Suite Strength parameter was removed. The Enable provided cipher suites parameter was introduced to display the list of enabled cipher suites.

Release	Modification
ArubaOS 8.7.0.0	TLS v1.2 is the default ssl-protocol in the Web-Server. TLS v1 and TLS v1.1 is disabled by default.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show websocket

```
show websocket
  clearpass
  debug
  state
  statistics
```

Description

Displays the ClearPass WebSocket configuration.

Parameter	Description
clearpass	Shows the ClearPass WebSocket profile.
debug	Shows the WebSocket interface debug information.
state	Shows the WebSocket connection state.
statistics	Shows the WebSocket Interface statistics.

Example

The output of the following command displays the ClearPass WebSocket profile.

```
(host) [mynode] #show websocket clearpass
ClearPass WebSocket Profile
-----
Parameter                               Value
-----
ClearPass WebSocket Interface           Enabled
Primary ClearPass Insight Server        10.4.174.104:443 apiadmin/*****
Secondary ClearPass Insight Server      10.4.174.105:443 apiadmin/*****
The output of the following command displays the WebSocket interface debug
information.
(host) [mynode] #show websocket debug clearpass
ClearPass WebSocket Interface Debug Information
-----
#Active-DevId-Table  #Working-Queue
-----
2                    1
```

The output of the following command displays the current connection state of the ClearPass WebSocket interface that is configured.

```
(host) [mynode] #show websocket state clearpass
```

```

ClearPass Web-Socket Connection State [Interface: Enabled]
-----
Server                               State
-----
Primary:   SECIRTY67.ACMECOMPANY.COM:443  DOWN
Secondary: 10.17.5.210:443                UP[08/22/16 13:38:50]Established

```

The output of this command includes the following parameters.

Parameter	Description
Server	Displays the primary and secondary ClearPass Insight server.
State	Displays the state of the primary and secondary ClearPass Insight server, which is either UP or DOWN.

The output of the following command displays the current statistics of ClearPass WebSocket interface.

```

(host) [mynode] #show websocket statistics clearpass

ClearPass WebSocket Interface Statistics Summary
-----
DevId Replayed  DevId Created  DevId Deleted  SUB Item Sent  SUB Msg Sent
UNSUB Item Sent  UNSUB Msg Sent  PUB Item Received  PUB Item Posted
-----
0                10             0               10             1              0
                0              0               0

```

The output of this command includes the following parameters.

Parameter	Description
DevId Replayed	Counter to track the number of device Ids replayed.
DevId Created	Counter to track the number of device Ids created.
DevId Deleted	Counter to track the number of device Ids deleted.
SUB Item Sent	When an interface is established, the existing device Ids are re-played and sent as sub items to ClearPass.
SUB Msg Sent	Counter to track the sub items that are consolidated and sent to ClearPass as sub messages.

Parameter	Description
UNSUB Item Sent	Counter to track the sub items sent to ClearPass, when ever a device Id is deleted.
UNSUB Msg Sent	Counter to track the deleted sub items consolidated as a sub message and sent to ClearPass.
PUB Item Received	When a subscribed profile for a specific station is updated in the ClearPass Insight server, a PUB message with the station's device profile information is sent back to the controller through the WebSocket connection. This event is mapped to the ArubaOS device type data.
PUB Item Posted	Counter to track the items successfully posted.

Related Commands

Command	Description
websocket clearpass	This command configures the ClearPass WebSocket profile. This command configures the primary and secondary ClearPass Insight server.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

show whitelist-db cpsec/show allowlist-db cpsec

```
show whitelist-db cpsec/show allowlist-db cpsec
  ap-group <ap_group>
  ap-name <ap_name>
  cert-type {factory-cert|switch-cert}
  mac-address <name>
  page <num>
  page-size <page-size>
  search-by
  sort-by
  sort-direction {ascending | descending}
  start <offset>
  state {approved-ready-for-cert|certified-factory-cert|unapproved-factory-
cert|unapproved-no-cert}
```

Description

Displays the campus AP whitelist/allowlist for campus APs using the control plane security feature. To view information for a single AP, use the command `show whitelist-db cpsec mac-address <mac-address>/ show allowlist-db cpsec mac-address <mac-address>`. If your deployment includes both Mobility Conductor and managed devices, then the campus AP whitelist/allowlist on every managed device contains an entry for every secure AP on the network, regardless of the managed device to which it is connected.

Parameter	Description
<code>ap-group <ap_group></code>	Specify the AP-Group name.
<code>ap-name <ap_name></code>	Specify the AP name.
<code>cert-type</code> <code>factory-cert switch-cert</code>	<ul style="list-style-type: none">▪ factory-cert: Use this parameter if AP is using a factory certificate.▪ switch-cert: Use this parameter if AP is using a certificate signed by the switch.
<code>mac-address <name></code>	MAC address of the campus AP you want to enter into the CPsec allowlist database.
<code>page <num></code>	ArubaOS CLI displays 50 whitelist/allowlist database entries per page. Filter the output of this command by displaying information starting at the specified page number.
<code>page-size <page-size></code>	Display number of records per page. The default value is 50 and a maximum of 500 records can be displayed per page.

Parameter	Description
search-by <searchstr>	Specify the string to search for.
sort-by	Specify the column by which the list is to be sorted.
sort-direction {ascending descending}	Sort the list in ascending or descending order.
start <offset>	Start displaying the table at the specified record in the database
state	Sort by one of the following AP states: <ul style="list-style-type: none"> ▪ approved-ready-for-cert: AP in Approved state and is ready to receive a certificate. ▪ certified-factory-cert: AP in Certified state and has a factory certificate. ▪ unapproved-factory-cert: AP in Unapproved state and has a factory certificate. ▪ unapproved-no-cert: AP in Unapproved state and has no or unknown certificate.

Example

The output of the following command shows the campus AP allowlist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host) #show whitelist-db cpsec mac-address 00:16:CF:AF:3E:E1 /show
allowlist-db cpsec mac-address 00:16:CF:AF:3E:E1

Control-Plane Security whitelist/allowlist-entry Details
-----
MAC-Address      AP-Group      AP-Name      Enable      State
-----
00:16:CF:AF:3E:E1  employee      ap-office1    Enabled     cert-cont-cert

Cert-Type      Description  Revoke Text  Last Updated
-----
switch-cert                                Fri Oct 16 01:21:09 2009

Whitelist/Allowlist Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
MAC-Address	MAC address of the campus AP.

Parameter	Description
Enable	Shows whether the campus AP has been enabled or disabled.
State	Shows the current state of the campus AP. <ul style="list-style-type: none"> ▪ unapproved-no-cert: AP has no certificate and is not approved. ▪ unapproved-factory-cert: AP has a preinstalled certificate that was not approved. ▪ approved-ready-for-cert: AP is valid, but is waiting to receive a certificate. ▪ certified-factory-cert: AP has an approved factory-installed certificate ▪ certified-controller-cert: AP has an approved certificate from the managed device. ▪ certified-hold-factory-cert: An AP is put in this state when the managed device thinks the AP has been certified with a factory certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be reapproved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised. ▪ certified-hold-controller-cert: An AP is put in this state when the managed device thinks the AP has been certified with a managed device certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be reapproved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised.
Cert-Type	Type of certificate used by the AP. <ul style="list-style-type: none"> ▪ switch-cert: AP received a certificate from the managed device ▪ factory-cert: AP has a factory-installed certificate
Description	If you included an optional description when you added the AP to the campus AP whitelist/allowlist, that description will appear here.
Revoke Text	If you included an optional revoke description when you manually revoked the AP, that description will appear here.
Last Updated	Date and time that the AP record was last updated in the database.

Related Commands

Command	Description
whitelist-db cpsec add / allowlist-db cpsec add	Configure the campus AP whitelist/allowlist for the control plane security feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db cpsec-seq/show allowlist-db cpsec-seq

show whitelist-db cpsec-seq/show allowlist-db cpsec-seq

Description

Display the current sequence number for the Mobility Conductor or managed device whitelists/allowlists. The current sequence number in the **Sequence Number Details** table shows the number of changes to the campus AP whitelist/allowlist made on this managed device. Each managed device compares its campus AP whitelist/allowlist against whitelists/allowlists on other managed devices every two minutes. If a managed device detects a difference, it will send its changes to the other managed devices on the network. If all other managed devices on the network have successfully received and acknowledged all whitelist/allowlist changes made on this managed device, every entry in the **sequence number** column in the managed device whitelist/allowlist will have the same value as the number displayed in the **Sequence Number Details** table. If a managed device in the Mobility Conductor or managed device whitelist/allowlist has a lower sequence number, that managed device may still be waiting to complete its update, or its update acknowledgment may not have yet been received.

Example

The output of the first command below shows that the campus AP whitelist/allowlist has been updated 3 times on Mobility Conductor. The second command shows the managed device list on Mobility Conductor, and verifies that both managed devices have received and acknowledged all three of these changes.

```
(host) #show whitelist/allowlist-db cpsec-seq
Sequence Number Details
-----
Table Name          Current Seq Number
-----
cpsec_whitelist/allowlist  3

Whitelist Entries: 97

(host) # show whitelist/allowlist-db cpsec-local-list
Registered Local controller Details
-----
MAC-Address          IP-Address  Sequence Number  Remote Sequence Number  NULL
Update Count
-----
00:0b:86:51:a5:4c  10.3.53.2   3                1
00:A0:C9:14:C8:29  10.3.53.4   3                0

Whitelist/allowlist Entries: 2
```

Related Commands

Command	Description
whitelist-db cpsec add / allowlist-db cpsec add	Configure the campus AP whitelist for the control plane security feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db cpsec-status/show allowlist-db cpsec-status

```
show whitelist-db cpsec-status/show allowlist-db cpsec-status
```

Description

Display aggregate status information APs in the campus AP whitelist/allowlist.

Example

The output of the following command shows current status information for all APs in the Campus AP whitelist/allowlist:

```
(host) #show whitelist-db cpsec-status /show allowlist-db cpsec-status

My Mac-Address          00:0c:29:54:fb:cb
My IP-Address           10.15.56.171
My IPv6-Address         2012::171
Master/Conductor IP-Address 10.15.56.171
Master/Conductor IPv6-Address 2012::171
Switch-Role             Master/Conductor
Seq-state               Seq-num sync init
IPv4 LMS List:
  0.0.0.0
  10.15.56.32
  10.15.56.43
  0.0.0.0
  0.0.0.0
IPv6 LMS List:
  2012::33
  2012::16
  2012::17
whitelist-sync/allowlist-sync is disabled

Entries in whitelist/allowlist database

Total entries:          25
Approved entries:      0
Unapproved entries:    9
Certified entries:     15
Certified hold entries: 1
Revoked entries:       0
Marked for deletion entries: 0
Current Sequence Number: 538
```

Related Commands

Command	Description
<u>whitelist-db cpsec add / allowlist-db cpsec add</u>	Add an AP entry to the campus AP allowlist/whitelist.
<u>whitelist-db cpsec del / allowlist-db cpsec del</u>	Remove an individual AP entry to the campus AP allowlist/whitelist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> . All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.7.0.0	The output of the command was modified to include the following fields: <ul style="list-style-type: none"> ▪ My IPv6-Address ▪ Master IPv6-Address ▪ IPv6 LMS List
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db cpsec-stats / show allowlist-db cpsec-stats

show whitelist-db cpsec-stats / show allowlist-db cpsec-stats {mac-addr <mac-addr>}

Description

This command displays the statistics of CPSEC allowlist/whitelist in an AP.

Parameter	Description
mac-addr <mac-addr>	Displays allowlist/whitelist entry of a specific AP.

Example

The output of the command displays the statistics of CPSEC allowlist/whitelist,

```
(host)[mynode] #show whitelist-db cpsec-stats/show allowlist-db cpsec-stats
whitelist/Allowlist Statistics:
LNotS = Local sent notify seq num;          MNotR = Master/Conductor recv
notify seq num;          LNotR = Local recv notify resp;
LFetS = Local sent fetch query req;        MP1LS = Master/Conductor sent
pendlist to Local;        MP1AS = Master/Conductor sent pendlist to all;
LP1R = Local recv pendlist;                LCpAS = Local sent cpsec add
entry;          LCpDS = Local sent cpsec del entry;
LCpUS = Local sent cpsec update entry;      LCpQS = Local sent cpsec query
entry;          LCpAR = Local recv cpsec add entry resp;
LCpDR = Local recv cpsec del entry resp;    LCpUR = Local recv cpsec update
entry resp;    LCpQR = Local recv cpsec query entry resp;
MMsgS = Master/Conductor sent cpsec msg to local; MFetS = Master/Conductor
sent fetch resp;          LFetS = Local recv fetch resp
Global Statistics
-----
LNotS  MNotR  LNotR  LFetS  MP1LS  MP1AS  LP1R  LCpAS  LCpDS  LCpUS  LCpQS
LCpAR  LCpDR  LCpUR  LCpQR  MMsgS  MFetS  LFetS
-----
0      6225   0      0      3      3      0      0      0      0      0
0      0      0      0      25     1      0
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The following changes were introduced: <ul style="list-style-type: none">All instances of <code>whitelist</code> have been replaced with

Release	Modification
	<p>allowlist.</p> <ul style="list-style-type: none"> All instances of <code>master</code> have been replaced with <code>conductor</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db rap / show allowlist-db rap

```
show whitelist-db rap / show allowlist-db rap
  apgroup <ap-group>
  apname <ap-name>
  export-css <filename>
  fullname <full-name>
  long
  mac-address <address>
  page <num>
  page-size <page-size>
  search-by
  sort-by
  sort-direction {ascending | descending}
  start <offset>
```

Description

View detailed information for the remote AP whitelist/allowlist database.

Parameter	Description
apgroup <ap-group>	Display specific AP-entries for this AP-group.
apname <ap-name>	Display specific AP-entry for this AP-name.
export-css	Export the remote AP white list/allowlist to a file in the managed device's /flash/config/ folder. This file can be given to a content security provider to manage the remote AP database.
fullname <full-name>	Display specific AP-entry for this full-name in the RAP whitelist/allowlist database.
long	Display additional debugging information about an entry in the RAP whitelist/allowlist, including when it was last updated, the sequence number for the update, and any flags for the entry.
mac-address <mac-addr>	Display a whitelist/allowlist entry for the specified RAP MAC address.
page	ArubaOS CLI displays 50 whitelist/allowlist database entries per page. Filter the output of this command by displaying information starting at the specified page number.
page-size <page-size>	Display number of records per page. The default value is 50 and a maximum of 500 records can be displayed per page.

Parameter	Description
search-by <searchstr>	Specify the string to search for.
sort-by	Specify the column by which the list is to be sorted.
sort-direction {ascending descending}	Sort the list in ascending or descending order.
start <offset>	Start displaying the table at the specified record in the database

Example

In the example below, the command output has been divided into two tables to fit on a single page of this document. In the CLI, this output would appear in a single, wide table.

```
(host) #show whitelist-db rap / show allowlist-db rap

AP-entry Details
-----
Name          AP-Group  AP-Name    Full-Name  Authen-Username
Revoke-Text   -----  -----    -----    -----
-----
00:0b:86:c3:58:38  local    AP-5B      chucks_AP  Dev\Sarah
00:0b:86:66:01:aa  default  AP-5C      upstairs   Dev          AP
invalid
00:1a:1e:c0:1b:e0  default  AP-99
00:0b:86:66:03:3f  default  LAB-AP     addtl_rap  Dev\Chris
00:0b:86:66:02:09  default  LAB-AP

AP_Authenticated  Description  Date-Added          Enabled  Remote-IP
-----
Authenticated    Provisioned  Thu Mar  5 21:25:36 2009  Yes     192.0.2.3
Authenticated    Provisioned  Wed Mar  4 20:16:16 2009  Yes     192.0.2.6
Authenticated    Provisioned  Tue May 19 07:53:29 2009  Yes     192.0.2.12
Authenticated    Provisioned  Fri May  8 10:37:40 2009  Yes     192.0.2.13

AP Entries: 5
```

The output of this command includes the following information:

Parameter	Description
Name	MAC address of the remote AP.

Parameter	Description
AP-Group	Name of the AP group to which the remote AP has been assigned.
AP-name	Name of the remote AP. If no name has been specified, this column will display the remote AP's MAC address
Full-name	Text string used to identify the remote AP. This field often describes the AP's user, and corresponds to the User Name field in the RAP whitelist in the WebUI.
Authen-Username	User name of the user who authenticated the remote AP. This parameter holds the user name of the user who authenticated the remote AP. This is related to the zero touch authentication feature, as a user needs to authenticate an AP before it gets its complete configuration. Before the AP is authenticated, it is given a restricted configuration to allow users to perform captive portal authorization via the remote AP's ENET ports to authenticate the remote AP. The username used during captive portal authentication will be stored in this field. This cannot be added manually when creating a local-userdb-ap entry.
Revoke-Text	The command allowlist/whitelist-db rap revoke includes an optional revoke-comment parameter that allows network administrators to explain why the remote AP was revoked. If a remote AP is revoked, and a revoke comment entered, this text appears in the revoke-text column in the <code>show allowlist/whitelist-db rap command</code> . When a local DB entry is reenabled via the command allowlist/whitelist-db rap modify mac-addr mode enable , this field is cleared.
AP_Authenticated	This column indicates the authorization status of the RAP. A RAP can either be Authenticated or Provisioned . Remote APs that <i>do not</i> support certificate-based provisioning will always display a Provisioned status. Remote APs that support certificate-based provisioning can display either a Authenticated or Provisioned status, depending on their configuration and authentication status. <ul style="list-style-type: none"> ■ If the remote AP has a defined AP authorization profile, the remote AP will be in a "Provisioned" state with a limited configuration until it is authenticated. After the remote AP has been authenticated, it will be in an "Authenticated" state. ■ If the remote AP does not have a defined AP authorization profile, the remote AP will be in a "Provisioned" state, but will still receive the full configuration assigned to that AP and its AP group.
Description	A text string used to further identify the remote AP.
Date-Added	Date and time that the AP was added to the local user database
Enabled	This column shows if the entry in the database is enabled or disabled. Database entries can be enabled or disabled using the CLI commands: <pre> allowlist/whitelist-db rap {add modify} mac-address <mac-addr> mode{enable disable} and allowlist/whitelist-db rap revoke mac-address <mac-addr> </pre>

Related Commands

Command	Description
whitelist-db rap add /allowlist-db rap add	Add, delete, modify or revoke remote AP entries in the current remote AP whitelist/allowlist table.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of whitelist have been replaced with allowlist .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show whitelist-db rap-local-switch-list/show allowlist-db rap-local-switch-list

```
show whitelist-db rap-local-switch-list [mac-address <mac-address>]
```

Description

Displays the remote AP whitelist/allowlist local switch list on Mobility Conductor. When you have remote APs on a network with both master/conductor and managed devices, Mobility Conductor maintains a whitelist/allowlist of managed devices with remote APs. When you change a remote AP whitelist/allowlist on any managed device, that managed device contacts Mobility Conductor to check the local switch whitelist/allowlist, then contacts every other managed device to notify it of the change. This allows a remote AP to move between managed devices and still stay connected to the secure network.

To view information for a single managed device, use the command `show whitelist-db rap-local-switch-list mac-address <mac-address>`. To view a list of all managed devices, use the command `show whitelist-db rap-local-switch-list`.

Parameter	Description
<code>mac-address <mac-address></code>	MAC address of the managed device whose data you want to view.

Example

The following command shows information for all managed devices in the managed device whitelist. The output in the example below has been divided into sections to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
(host) #show whitelist-db rap-local-switch-list

Active   MAC-Address           IP-Address           Sequence Number     Remote Sequence
Number
-----
-----
1         00:0b:86:51:a5:4c    10.3.53.2           3                    1
1         00:A0:C9:14:C8:29    10.3.53.4           3                    0

NULL Update Count      Local Purge  Remote Purge  Remote Last-Seq  Last Update
Sent
-----
--
0                 0            0            2                Mon May 4 13:33:29 2013
0                 0            0            2                Mon May 4 13:32:55 2013
```

```

Last Update Received
-----
Mon May 4 13:33:18 2013
Mon May 4 13:32:19 2013W

Whitelist Entries: 2

```

The output of this command includes the following information:

Parameter	Description
Active	Shows if the managed device is active on the network. <ul style="list-style-type: none"> ▪ 1: Active ▪ 0: Inactive
MAC-Address	MAC address of the managed device.
IP-Address	IP address of the managed device.
Sequence Number	The number of times the managed device in the whitelist/allowlist received and acknowledged a remote AP whitelist/allowlist change from Mobility Conductor. In the example above, both managed devices received and acknowledged three remote AP whitelist/allowlist changes sent from Mobility Conductor.
Remote Sequence Number	The number of times that Mobility Conductor has received and acknowledged a remote AP whitelist/allowlist change from the managed device in the whitelist/allowlist. In the example above, Mobility Conductor received and acknowledged a single remote AP whitelist/allowlist change from the managed device with the MAC address 00:0b:86:51:a5:4c.
Null Update Count	The number of times the managed device has checked its remote AP whitelist/allowlist and found nothing to synchronize with the remote managed device. By default, the managed device compares its remote AP whitelist/allowlist against whitelist/allowlist on other managed devices every minute. If the null update count reaches 5, the managed device will send an "empty sync" heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description
<u>show whitelist-db rap-master-switch-list/show allowlist-db rap-local-switch-list</u>	Delete a Mobility Conductor from the Mobility Conductor table used by the remote AP whitelist/allowlist
<u>whitelist-db rap del / allowlist-db rap del</u>	Remove an AP entry from the remote AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db rap-master-switch-list/show allowlist-db rap-local-switch-list

```
show whitelist-db rap-master-switch-list [mac-address <mac-address>]/show  
allowlist-db rap-local-switch-list [mac-address <mac-address>]
```

Description

Displays the remote AP whitelist/allowlist master/conductor switch list on managed devices with remote APs. When your network has both master/conductor and managed devices, each managed device with associated remote APs has a master/conductor switch whitelist/allowlist which contains the IP and MAC addresses of Mobility Conductor. If your network has a redundant Mobility Conductor, then this list will contain more than one entry.

To view information for a single Mobility Conductor, use the command `show whitelist-db rap-master-switch-list mac-address <mac-address>/show allowlist-db rap-local-switch-list mac-address <mac-address>`. To view a list of all Mobility Conductors, use the command `show whitelist-db rap-master-switch-list/show allowlist-db rap-local-switch-list`.

Parameter	Description
mac-address <mac-address>	MAC address of the managed device whose data you want to view.

Example

The following command shows that the managed devices have a single Mobility Conductor with the IP address 192.0.2.143. The output in the example below has been divided into sections to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
Active Sequence  MAC-Address          IP-Address          Sequence Number    Remote  
-----  
1           00:0b:86:51:a5:4c    192.0.2.14         2                   2  
  
NULL Update Count  Local Purge  Remote Purge  Remote Last-Seq  Last Update  
Sent  
-----  
0           0           0           1                Mon May 4 12:44:24  
0  
  
Last Update Received  
-----
```



```
Mon May 4 12:44:20
```

```
Whitelist Entries: 1
```

The output of this command includes the following information:

Parameter	Description
Active	Shows if the controller is active on the network. <ul style="list-style-type: none">▪ 1: Active▪ 0: Inactive
MAC-Address	MAC address of Mobility Conductor.
IP-Address	IP address of Mobility Conductor.
Sequence Number	The number of times the Mobility Conductor in the whitelist/allowlist received and acknowledged a remote AP whitelist/allowlist change from the managed device. In the example above, the Mobility Conductors received and acknowledged three remote AP whitelist/allowlist changes sent from a managed device.
Remote Sequence Number	The number of times that the managed device has received and acknowledged a remote AP whitelist/allowlist change from the Mobility Conductor in the whitelist/allowlist.
Null Update Count	The number of times the managed device has checked its remote AP whitelist/allowlist and found nothing to synchronize with the remote managed device. By default, the managed device compares its remote AP whitelist/allowlist against whitelist/allowlist on other managed devices every minute. If the null update count reaches 5, the managed device will send an "empty sync" heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description
<u>whitelist-db rap-local-switch-list/allowlist-db rap-local-switch-list</u>	Delete a managed device from the local switch table used by the remote AP whitelist/allowlist
<u>whitelist-db rap del / allowlist-db rap del</u>	Remove an AP entry from the remote AP whitelist/allowlist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db rap-status / show allowlist-db rap-status

show whitelist-db rap-status / show allowlist-db rap-status

Description

Display aggregate status information APs in the remote AP whitelist/allowlist.

Example

The output of the following command shows current status information for all APs in the remote AP whitelist/allowlist:

```
(host) #show whitelist-db rap-status / show allowlist-db rap-status
Entries in whitelist/allowlist database

Total entries:                41
Revoked entries:              1
Marked for deletion entries:  0
```

The output of this command includes

Parameter	Description
Total entries	Total number of entries in the remote AP whitelist/allowlist.
Revoked entries	Number of remote APs whose entries have been revoked.
Marked for deletion entries	Number of remote APs whose entries have been marked for deletion. An entry will not be permanently deleted until all other managed devices on the network acknowledge the deletion.

Related Commands

Command	Description
show whitelist-db rap-master-switch-list/show allowlist-db rap-local-switch-list	Display the list of Mobility Conductors /Mobility Conductors with remote APs managed using the remote AP whitelist/allowlist.

Command	Description
show whitelist-db rap-local-switch-list/show allowlist-db rap-local-switch-list	Display the list of managed devices with remote APs managed using the remote AP whitelist/allowlist.
show whitelist-db rap / show allowlist-db rap	View detailed information for the remote AP allowlist/whitelist database.
whitelist-db rap add /allowlist-db rap add	Add an AP entry to the remote AP allowlist/whitelist.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show whitelist-db seq-pendlist / show allowlist-db seq-pendlist

`show whitelist-db seq-pendlist / show allowlist-db seq-pendlist`

Description

Displays the aggregate maximum pending list information.

Example

The output of the following command shows the maximum pending list information:

```
(host) #show whitelist-db seq-pendlist / show allowlist-db seq-pendlist
Maximum Sequence number in seq pendlist:    0
```

Related Commands

Command	Description
whitelist-db cpsec add / allowlist-db cpsec add	Configure the campus AP allowlist/whitelist for the control plane security feature.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wired-blacklist-clients/show wired-denylist-clients

show wired-blacklist-clients/show wired-denylist-clients

Description

This command shows wired clients that are blacklisted/denylisted. Issue this command to list the blacklisted/denylisted wired clients.

Examples

```
(host) [mynode] (config)#show wired-blacklist-clients
/show wired-denylist-clients
```

The output of this command is as follows:

```
Wired user Blacklist/Denylist table
-----
MAC  AP name  Slot/Port  Reason  Blacklist/Denylist Time (Sec)
---  -
b4:b5:2f:8d:cc:96  ac:a3:1e:cd:36:84  0/1          session-blacklist/session-
denylist  258
```

Related Commands

Command	Description
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.

Command History

Version	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan

```
show wlan
  6ghz-rrm-ie-profile
  anyspot-profile
  bcn-rpt-req-profile
  client-wlan-profile
  dot11k-profile
  dot11r-profile
  edca-parameters-profile
  he-ssid-profile
  hotspot
  ht-ssid-profile
  mu-edca-parameters-profile
  rrm-ie-profile
  sae-profile
  ssid-profile
  traffic-management-profile
  tsm-req-profile
  virtual-ap
  wmm-traffic-management-profile
```

Description

This command displays the list of all WLAN profiles. Click the parameter links below to view the corresponding show commands.

Parameter	Description
6ghz-rrm-ie-profile	Displays RRM IE Profile for 6 GHz.
anyspot-profile	Displays anyspot profile.
bcn-rpt-req-profile	Displays Beacon Report Request frames.
client-wlan-profile	Displays WLAN profile configuration for a VIA client.
dot11k-profile	Displays a list of all 802.11k profiles.
dot11r-profile	Displays a list of all 802.11r profiles.
edca-parameters-profile	Displays an EDCA profile for APs or for clients (stations).
he-ssid-profile	Displays the configurations of a high-efficiency SSID profile.
hotspot	Displays Hotspot 2.0 profile settings.
ht-ssid-profile	Displays high-throughput SSID profile settings.

Parameter	Description
mu-edca-parameters-profile	Displays MU EDCA Parameters profile settings.
rrm-ie-profile	Displays RRM IE profile settings.
sae-profile	Displays WPA3 SAE configuration profile settings.
ssid-profile	Displays SSID profile settings.
traffic-management-profile	Displays Traffic management profile settings.
tsm-req-profile	Displays TSM Report Request profile settings.
virtual-ap	Displays Virtual AP profile settings.
wmm-traffic-management-profile	Displays WMM traffic management profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan 6ghz-rrm-ie-profile

```
show wlan 6ghz-rrm-ie-profile [<profile-name>]
```

Description

Shows a list of all 6GHz RRM IE profiles, or display detailed configuration information for a specific profile. Use this command without the <profile> parameter to display the 6GHz RRM IE profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an 6GHz RRM IE profile.

Examples

The following example shows one 6GHz RRM IE profile configured on the controller.

The **References** column lists the number of other profiles with references to the 6GHz RRM IE profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host)[mynode] #show wlan 6ghz-rrm-ie-profile

RRM IE Profile for 6GHz List
-----
Name       References  Profile Status
-----
default   1
Total:1
```

The following example shows configuration settings defined for the profile **default**:

```
(host)[mynode] #show wlan 6ghz-rrm-ie-profile default

RRM IE Profile for 6GHz "default"
-----
Parameter                                     Value
-----
Advertise Enabled Capabilities IE             Enabled
Advertise Country IE                           Enabled
Advertise Power Constraint IE                  Enabled
Advertise TPC Report IE                        Enabled
Advertise QBSS Load IE                         Enabled
Advertise BSS AAC IE                           Enabled
Advertise Quiet IE                             Enabled
```

Related Commands

Command	Description
wlan dot11k-profile	Configure a 802.11k radio profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show wlan anyspot-profile

```
show wlan anyspot-profile [<profile-name>]
```

Description

The output of this command displays configuration settings for a WLAN anyspot profile. The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks. Use this command without the <profile> parameter to display the entire anyspot profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an anyspot profile.

Example

The following command displays configuration information for an active (enabled) anyspot profile with two excluded ESSIDs, and one preset ESSID.

```
(host) [mynode] #show wlan anyspot-profile default
Anyspot profile "default"
-----
Parameter                               Value
-----
Enable Anyspot                           true
Exclude ESSID(s) (exact match)           corp_dev_1
Exclude ESSID(s) (exact match)           corp_voip_1
Exclude ESSID(s) (containing string(s))  N/A
Preset ESSID(s)                           corpGuest
```

The output of this command displays the following parameters:

Parameter	Description
enable-anyspot	Indicates if the anyspot feature is enabled or disabled.
exclude-ssid <exclude-ssid>	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the Exclude ESSID lists. ESSIDs from neighboring APs will automatically appear in this list as long as the anyspot-enabled AP can detect that ESSID.

Parameter	Description
<code>exclude-wildcard <exclude-wildcard></code>	An anyspot-enabled radio will not respond to client probe requests using an ESSID that matches a string in the Exclude ESSID (containing string) list .
<code>preset-ssid <preset-ssid></code>	If a client sends a probe request without an ESSID (that is, the probe request is not looking for a specific network) then the anyspot-enabled AP will respond to the probe request with an ESSID from this list.

Related Commands

Command	Description
<code>wlan anyspot-profile</code>	The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan bcn-rpt-req-profile

```
show wlan bcn-rpt-req-profile <profile-name>
```

Description

Shows configuration and other information about the parameters for the Beacon Report Request frames. Use this command without the <profile> parameter to display the entire Beacon Report Request profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile. For this profile to take effect, the 802.11K feature needs to be enabled.

Parameter	Description
<profile-name>	Name of a WLAN beacon report request profile.

Example

The following command displays configuration information for the Beacon Report Request frames:

```
(host)(mynode) #show wlan bcn-rpt-req-profile
Beacon Report Request Profile List
-----
Name      References  Profile Status
----      -
default   1
test      0
Total:2
(host) #
(host) #show wlan bcn-rpt-req-profile default

Beacon Report Request Profile "default"
-----
Parameter                               Value
-----
Interface                                 1
Regulatory Class                          12
Channel                                   9
Randomization Interval                    100
Measurement Duration                       100
Measurement Mode for Beacon Reports        active-all-ch
Reporting Condition                         2
ESSID Name                                aruba-ap
Reporting Detail                           Disabled
Measurement Duration Mandatory             Disabled
Request Information values                  0/21/22
```

The output of this command includes the following parameters:

Parameter	Description
Interface	Specifies the Radio interface for transmitting the Beacon Report Request frame. It can have a value of either 0 or 1.
Regulatory Class	Specifies the Regulatory Class field in the Beacon Report Request frame.
Channel	Specifies the Channel field in the Beacon Report Request frame.
Randomization Interval	Specifies the Randomization Interval field in the Beacon Report Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units).
Measurement Duration	Specifies the Measurement Duration field in the Beacon Report Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs.
Measurement Mode for Beacon Reports	Specifies the mode used for the measurement. The valid measurement modes are: <ul style="list-style-type: none"> ▪ active-all-ch ▪ active-ch-rpt ▪ beacon-table ▪ passive
Reporting Condition	Specifies the value for the "Reporting Condition" field in the Beacon Reporting Information sub-element present in the Beacon Report Request frame.
ESSID Name	Specifies the value for the "SSID" field in the Beacon Report Request frame.
Reporting Detail	Indicates the value for the "Detail" field in the Reporting Detail sub-element present in the Beacon Report Request frame.
Measurement Duration Mandatory	Specifies the "Duration Mandatory" bit of the Measurement Request Mode field of the Beacon Report Request frame.
Request Information values	Indicates the contents of the Request Information IE that could be present in the Beacon Report Request frame. The Request Information IE is present for all Measurement Modes except the 'Beacon Table' mode. It consists of a list of Element IDs that should be included by the client in the response frame.

Related Commands

Command	Description
wlan bcn-rpt-req-profile	Configures a Beacon Report Request Profile to provide the parameters for the Beacon Report Request frames.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan client-wlan-profile

```
show wlan client-wlan-profile <profile-name>
```

Description

This command shows a WLAN profile configuration for a VIA client. The optional output modifiers begin, exclude, and include help you display those lines that begin, include, and exclude respectively, the line expression given in the CLI command. The redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	Name of the WLAN profile.

Example

The following command displays WLAN profile configuration for a VIA client:

```
(host)[mynode] #show wlan client-wlan-profile
VIA Client WLAN Profile List
-----
Name   References  Profile Status
----  -

```

Related Commands

Command	Description
wlan client wlan-profile	This command is used to configure WLAN client WLAN profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan dot11k-profile

```
show wlan dot11k-profile [<profile-name>]
```

Description

Shows a list of all 802.11k profiles, or display detailed configuration information for a specific 802.11k profile. Use this command without the <profile> parameter to display the 802.11k profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an 802.11k profile.

Examples

The following example shows two 802.11k profiles configured on the controller.

The **References** column lists the number of other profiles with references to the 802.11k profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host)[mynode] #show wlan dot11k-profile

802.11K Profile List
-----
Name                               References  Profile Status
----                               -
default                             8
11kprofile2                          1
Total: 2
```

The following example shows configuration settings defined for the profile **default**:

```
(host)[mynode] #show wlan dot11k-profile default

802.11K Profile "default"
-----
Parameter                               Value
-----
-
Advertise 802.11K Capability              Disabled
Forcefully disassociate on-hook voice clients Disabled
```

```

Measurement Mode for Beacon Reports
beacon-table
Configure specific channel for Beacon Requests
Disabled
Channel requested for Beacon Reports in 'A' band 36
Channel requested for Beacon Reports in 'BG' band 1
Time duration between consecutive Beacon Requests 60
sec
Time duration between consecutive Link Measurement Requests 60
sec
Time duration between consecutive Transmit Stream Measurement Requests 90
sec

```

The output of this command includes the following data columns:

Parameter	Description
Advertise 802.11k Capability	Shows if the profile has enabled or disabled the 802.11K feature.
Forcefully disassociate on-hook voice clients	If enabled, the AP may forcefully disassociate clients that reach the maximum CAC peak capacity or call handoff reservation.
Measurement Mode for Beacon Reports	Shows the profile's beacon measurement mode: <ul style="list-style-type: none"> ▪ active: In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ▪ beacon-table: In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode. ▪ passive: In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report.

Related Commands

Command	Description
wlan dot11k-profile	Configure a 802.11k radio profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Enable and Config modes on Mobility Conductor and managed devices.

show wlan dot11r-profile

show wlan dot11r-profile [<profile>]

Description

Shows a list of all 802.11r profiles, or display detailed configuration information for a specific 802.11r profile. Use this command without the <profile> parameter to display the 802.11r profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile>	Name of an 802.11r profile.

Examples

The following example shows that the controller has two configured 802.11r profiles.

The **References** column lists the number of other profiles with references to the 802.11r profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host)[mynode] #show wlan dot11r-profile

802.11r Profile List
-----
Name                References  Profile Status
----                -
default             8
voice-enterprise    1

Total: 2
```

The following example shows configuration settings defined for the profile **default**:

```
(host)[mynode] #show wlan dot11r-profile default
802.11r Profile "default"
-----
Parameter                Value
-----
Advertise 802.11r Capability  Disabled
802.11r Mobility Domain ID   1
802.11r R1 Key Duration     3600
802.11r R1 Key Assignment    dynamic
```

The output of this command includes the following data columns:

Parameter	Description
Advertise 802.11r Capability	Shows if the profile has enabled or disabled the 802.11r feature.
802.11r Mobility Domain ID	Shows the unique ID that identifies the mobility domain.
802.11r R1 Key Duration	Shows the r1 key timeout value in seconds for decrypt-tunnel or bridge mode.
802.11r R1 Key Assignment	Shows if the r1 key assignment is static or dynamic.

Related Commands

Command	Description
wlan dot11r-profile	This command configures an 802.11r radio profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan edca-parameters-profile

```
show wlan edca-parameters-profile ap|station [<profile>]
```

Description

Displays an EDCA profile for APs or for clients (stations). EDCA profiles are specific either to APs or clients. Use this command without the <profile> parameter to display a EDCA Parameters profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile>	Name of a EDCA Parameters profile.

Examples

The following example shows that the controller has three EDCA Parameters profiles configured for stations. The **References** column lists the number of other profiles with references to the EDCA Parameters profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host)[mynode] #show wlan edca-parameters-profile station
EDCA Parameters profile (Station) List
-----
Name           References  Profile Status
----           -
station-corp1  3
station-corp2  1
testprofile    0

Total:3
```

The following example shows configuration settings defined for the profile **station-corp1**:

```
(host)[mynode] #show wlan edca-parameters-profile ap station-corp1
EDCA Parameters
-----
AC           ECWmin  ECWmax  AIFSN  TXOP  ACM
--           -
Best-effort  4       6       3       0     0
Background  4       10      7       0     0
Video       3       4       1       94    0
Voice       2       3       1       47    0
```

The output of this command includes the following data columns:

Parameter	Description
AC	Name of an Access channel queue (Best-effort, Background, Video, or Voice).
ECWmin	The exponential (n) value of the minimum contention window size, as expressed by $2^n - 1$. A value of 4 computes to $2^4 - 1 = 15$.
ECWmax	The exponential (n) value of the maximum contention window size, as expressed by $2^n - 1$. A value of 4 computes to $2^4 - 1 = 15$.
AIFSN	Arbitrary inter-frame space number.
TXOP	Transmission opportunity, in units of 32 microseconds.
ACM	If this column displays a 1, the profile has enabled mandatory admission control. If this column displays a 0, the profile has disabled this feature.

Related Commands

Command	Description
wlan ssid-profile	This command configures an SSID profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	This show command is available in the base operating system, but the controller must have the PEFNG license in order to configure EDCA Parameter Profiles.	Config or Enable mode on Mobility Conductor.

show wlan he-ssid-profile

```
show wlan he-ssid-profile <profile-name>
```

Description

This command shows the configurations of a high-efficiency SSID profile. The optional output modifiers begin, exclude, and include help you display those lines that begin, include, and exclude respectively, the line expression given in the CLI command. The redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	Name of the high-efficiency ssid profile.

Example

```
(host)[mynode] #show wlan he-ssid-profile default
High-efficiency SSID profile "default"
-----
Parameter Value
-----
High efficiency enable (SSID) Enabled
Dynamic fragmentation level Level-0
HE duration based RTS 1023
Individual TWT Enabled
HE TXBF Enabled
HE Supported MCS map 11,11,11,11,11,11,11,11
HE MU-OFDMA Enabled
HE MU-MIMO Enabled
HE UL MU-MIMO Enabled
HE Guard Interval 800ns 1600ns 3200ns
-----
default 2
Total:1
```

Related Commands

Command	Description
wlan he-ssid-profile	This command configures wlan he-ssid profile.

Command History

Version	Modification
ArubaOS 8.8.0.0	The output was modified to include the status of HE UL MU-MIMO transmission.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot

```
show wlan hotspot
  advertisement-profile
  anqp-3gpp-nwk-profile
  anqp-domain-name-profile
  anqp-ip-addr-avail-profile
  anqp-nai-realm-profile
  anqp-nwk-auth-profile
  anqp-roam-cons-profile
  anqp-venue-name-profile
  h2qp-conn-capability-profile
  h2qp-op-cl-profile
  h2qp-operator-friendly-name-profile
  h2qp-osu-prov-list-profile
  h2qp-wan-metrics-profile
  hs2-profile
```

Description

This command displays the Hotspot 2.0 configuration profiles. Click the parameter links below to view the corresponding show commands.

Parameter	Description
advertisement-profile	Displays WLAN ANQP advertisement profile settings.
anqp-3gpp-nwk-profile	Displays 3GPP Cellular Network profile configuration settings.
anqp-domain-name-profile	Displays WLAN ANQP Domain Name profile settings.
anqp-ip-addr-avail-profile	Displays WLAN ANQP IP Address Availability profile settings.
anqp-nai-realm-profile	Displays WLAN ANQP Network Access Identifier (NAI) Realm profile settings.
anqp-nwk-auth-profile	Displays WLAN ANQP network authentication profile settings.
anqp-roam-cons-profile	Displays ANQP Roaming Consortium profile settings.
anqp-venue-name-profile	Displays ANQP Venue Name profile settings.
h2qp-conn-capability-profile	Displays H2QP connection capability profile settings.
h2qp-op-cl-profile	Displays H2QP operating class profile settings.
h2qp-operator-friendly-name-profile	Displays H2QP operator-friendly name profile settings.
h2qp-osu-prov-list-profile	Displays H2QP OSU providers list profile settings.

Parameter	Description
h2qp-wan-metrics-profile	Displays H2QP WAN metrics profile settings.
hs2-profile	Displays Hotspot 2.0 profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan hotspot advertisement-profile

show wlan hotspot advertisement-profile [<profile-name>]

Description

The output of this command displays settings for a WLAN ANQP advertisement profile. ANQP profiles and H2QP profiles define the 802.11u IEs to be broadcast by an 802.11u capable AP. Use this command to view the ANQP and H2QP profiles to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP advertisement profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of a wlan hotspot advertisement profile.

Examples

The following example shows that the controller has two configured advertisement profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] #show wlan hotspot advertisement-profile
Advertisement Profile List
-----
Name           References  Profile Status
----           -
default        1
Westgate_Mall  2
Total:2.
```

This example displays the configuration settings for the profile **Wireless_rf_profile**.

```
(host)[mynode] (config) #show wlan hotspot advertisement-profile Wireless_
rf_profile
Advertisement Profile "default"
-----
Parameter                               Value
-----
ANQP Venue Name Profile                  venue_mall
ANQP Network Authentication Profile      auth1
ANQP Roaming Consortium Profile          default
```

```

ANQP NAI Realm Profile           Realm2
ANQP 3GPP Cellular Network Profile default
ANQP IP Address Availability Profile ipv4_Profile
H2QP WAN Metrics Profile         default
H2QP Operator Friendly Name Profile default
H2QP Connection Capability Profile default
H2QP Operating Class Indication Profile default
ANQP Domain Name Profile         corp_domain

```

The output of this command includes the following parameters:

Parameter	Description
ANQP Venue Name Profile	Name of the ANQP Venue Name profile associated with this WLAN advertisement profile.
ANQP Network Authentication Profile	Name of the ANQP Network Authentication profile associated with this WLAN advertisement profile.
ANQP Roaming Consortium Profile	Name of the ANQP Roaming Consortium profile associated with this WLAN advertisement profile.
ANQP NAI Realm Profile	Name of the ANQP NAI Realm profile associated with this WLAN advertisement profile.
ANQP 3GPP Profile	Name of the ANQP 3GPP Cellular Network profile associated with this WLAN advertisement profile.
ANQP IP Address Availability Profile	Name of the ANQP IP Address Availability profile associated with this WLAN advertisement profile.
H2QP WAN Metrics Profile	Name of the H2QPWAN Metrics profile associated with this WLAN advertisement profile.
H2QP Operator Friendly Name Profile	Name of the H2QP Operator Friendly Name profile associated with this WLAN advertisement profile.
H2QP Connection Capability Profile	Name of the H2QP Connection Capability profile associated with this WLAN advertisement profile.
H2QP Operating Class Indication Profile	Name of the H2QP Operating Class Indication profile associated with this WLAN advertisement profile.

Parameter	Description
ANQP Domain Name Profile	Name of the ANQP domain name profile associated with this WLAN advertisement profile.

Related Commands

Command	Description
ntp	This command configures a WLAN advertisement profile for an 802.11u public access service provider.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-3gpp-nwk-profile

```
show wlan hotspot anqp-3gpp-nwk-profile [<profile-name>]
```

Description

This profile shows the configuration settings for a 3GPP Cellular Network profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command without the <profile> parameter to display the entire list of 3GPP profiles, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

The 3GPP Cellular Network Profile defines an ANQP IE to be sent in a GAS query response from an AP in a hotspot with a roaming relationship with a cellular operator. The 3GPP mobile country code and the 12-bit Mobile Network Code data in the IE can help the client select a 3GPP network.

Values configured in this profile will not be sent to clients unless you:

Associate the 3GPP Cellular Network profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-3gpp-nwk-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within the Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of a 3GPP Cellular Network profile.

Examples

The following example shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] (config)#show wlan hotspot anqp-3gpp-nwk-profile
ANQP 3GPP Cellular Network Profile List
-----
Name           References  Profile Status
----           -
default        1
Updated_PLMN   2
Total:2.
```

This example displays the configuration settings for the profile **Updated_PLMN**.

```
(host)[mynode] (config)#show wlan hotspot anqp-3gpp-nwk-profile Updated_PLMN
ANQP 3GPP Cellular Network Profile "Updated_PLMN"
```

```
-----
Parameter                               Value
-----
ANQP 3GPP network profile enable       Enabled
3GPP PLMN1                             310026
3GPP PLMN2                             208000
3GPP PLMN3                             208001
3GPP PLMN4                             N/A
3GPP PLMN5                             N/A
3GPP PLMN6                             N/A
```

The output of this command includes the following parameters:

Parameter	Description
ANQP 3GPP network profile enable	Shows if this profile has been enabled ANQP 3GPP Cellular Network profiles are disabled by default.
3gpp PLMN1	The Public Land Mobile Networks (PLMN) value of the highest-priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp PLMN2	The Public Land Mobile Networks (PLMN) value of the second-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp PLMN3	The Public Land Mobile Networks (PLMN) value of the third-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp PLMN4	The Public Land Mobile Networks (PLMN) value of the fourth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp PLMN5	The Public Land Mobile Networks (PLMN) value of the fifth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp PLMN6	The Public Land Mobile Networks (PLMN) value of the sixth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).

Related Commands

Command	Description
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-domain-name-profile

```
show wlan hotspot anqp-domain-name-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Domain Name profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the `<profile>` parameter to display the entire ANQP Domain Name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

Associate the 3GPP Cellular Network profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-3gpp-nwk-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within the Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<code><profile-name></code>	Name of a Domain Name profile.

Examples

The following example shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] #show wlan hotspot anqp-domain-name
ANQP Domain Name Profile List
-----
Name           References  Profile Status
----           -
corp_domain    2
default        1
Total:2.
```

This example displays the configuration settings for the profile **corp_domain**.

```
(host) [mynode] #show wlan hotspot anqp-domain-name-profile corp_domain
```

```

ANQP Domain Name Profile "corp_domain"
-----
Parameter      Value
-----
Domain Name    example.com

```

The output of this command includes the following parameters:

Parameter	Description
Domain Name	Domain name of the hotspot operator.
Profile List	List of available profiles.

Related Commands

Command	Description
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-ip-addr-avail-profile

```
show wlan hotspot anqp-ip-addr-avail-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP IP Address Availability profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP IP Address Availability profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP IP Address Availability profile with an ANQP advertisement profile. (wlan hotspot advertisement profile <profile-name> anqp-ip-addr-avail-profile <profile-name>)

Associate the ANQP advertisement profile with a Hotspot profile. (wlan hotspot h2-profile advertisement-profile <profile-name>)

Enable the hotspot feature within the Hotspot profile. (wlan hotspot h2-profile <profile-name> hotspot-enable)

Parameter	Description
<profile-name>	Name of an IP Address Availability profile.

Examples

The following example shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] # show wlan hotspot anqp-ip-addr-avail-profile
ANQP IP Address Availability Profile List
-----
Name           References  Profile Status
----           -
default        0
ipv4_Profile   2
ipv6_profile   1
Total:3.
```

The following example displays the configuration settings for the profile **ipv4_Profile**.

```
(host)[mynode] #show rf anqp-ip-addr-avail-profile ipv4_Profile
ANQP IP Address Availability Profile "ipv4_Profile"
-----
Parameter                               Value
-----
IPv4 Address Availability Type          public
IPv6 Address Availability Type          not-available
```

The output of this command includes the following parameters:

Parameter	Description
IPv4 Address Availability Type	<p>Indicates the availability of an IPv4 network. This parameter can display any of the following values:</p> <ul style="list-style-type: none"> ▪ availability-unknown: Network availability cannot be determined. ▪ not-available : Network is not available. ▪ port-restricted : Network has some ports restricted (for example, the network blocks port 110 to restrict POP mail). ▪ port-restricted-double-nated : Network has some ports restricted and multiple routers performing network address translation. ▪ port-restricted-single-nated : Network has some ports restricted and a single router performing network address translation. ▪ private-double-nated : Network is a private network with multiple routers doing network address translation. ▪ private-single-nated : Network is a private network a single router doing network address translation. ▪ public : Network is a public network
IPv6 Address Availability Type	<p>Indicates the availability of an IPv6 network. This parameter can display any of the following values:</p> <ul style="list-style-type: none"> ▪ available : An IPv6 network is available. ▪ availability-unknown: Network availability cannot be determined. ▪ not-available : Network is not available.

Related Commands

Command	Description
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-nai-realm-profile

```
show wlan hotspot anqp-nai-realm-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Network Access Identifier (NAI) Realm profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP NAI Realm profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP NAI Realm profile with an ANQP advertisement profile. (wlan hotspot advertisement profile <profile-name> anqp-nai-realm-profile <profile-name>)

Associate the ANQP advertisement profile with a Hotspot profile. (wlan hotspot h2-profile advertisement-profile <profile-name>)

Enable the hotspot feature within the Hotspot profile. (wlan hotspot h2-profile <profile-name> hotspot-enable)

Parameter	Description
<profile-name>	Name of an NAI Realm profile.

Examples

The following example shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] # show wlan hotspot anqp-nai-realm-profile

ANQP NAI Realm Profile List
-----
Name       References  Profile Status
-----
default    0
Realm1     2Realm2    2

Total:3.
```

The following example shows the configuration settings for the profile **Realm2**.

```
(host)[mynode] #show wlan hotspot anqp-nai-realm-profile Realm2
ANQP NAI Realm Profile "Realm2"
-----
Parameter                               Value
-----
NAI Realm name                           example.com
NAI Realm EAP Method                      eap-ttls
NAI Realm Authentication Parameter Type   expanded-eap
```

The output of this command includes the following parameters:

Parameter	Description
NAI Realm name	Name of the NAI realm. The realm name is often the domain name of the service provider.
NAI Realm EAP Method	The NAI Realm Authentication types sent as an ANQP IE in an GAS response.
NAI Realm Authentication Parameter Type	The EAP authentication method supported by the hotspot realm.

Related Commands

Command	Description
wlan hotspot anqp-nai-realm-profile	This command defines a Network Access Identifier (NAI) realm whose information can be sent as an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-nwk-auth-profile

show wlan hotspot anqp-nwk-auth-profile [<profile-name>]

Description

The output of this command displays settings for a WLAN ANQP network authentication profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP NAI Realm profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an ANQP Network Authentication profile.

Examples

The following example shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode] # show wlan hotspot anqp-nwk-auth-profile

ANQP Network Authentication Profile List
-----
Name           References  Profile Status
----           -
auth1          0
default        0

Total:2.
```

The following example displays the configuration settings for the profile **default**:

```
(host)[mynode] #show wlan hotspot anqp-nwk-auth-profile default

ANQP Network Authentication Profile "default"
-----
Parameter           Value
-----
Type of Network Authentication  acceptance
```

Redirect URL

N/A

The output of this command includes the following parameters:

Parameter	Description
Type of Network Authentication	Network Authentication Type being used by the hotspot network. This parameter can be any of the following values: <ul style="list-style-type: none">■ acceptance: Network requires the user to accept terms and conditions.■ dns-redirection: Additional information on the network is provided through DNS redirection.■ http-https-redirection : Additional information on the network is provided through HTTP/HTTPS redirection.■ online-enroll : Network supports online enrollment.
Redirect URL	If information on the network is provided through DNS redirection, this parameter displays the redirection URL.

Related Commands

Command	Description
wlan hotspot anqp-nwk-auth-profile	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-roam-cons-profile

```
show wlan hotspot anqp-roam-cons-profile [<profile>]
```

Description

The output of this command displays settings for a WLAN ANQP Roaming Consortium profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP Roaming Consortium profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Roaming Consortium profile with an ANQP advertisement profile. (wlan hotspot advertisement profile <profile-name> anqp-roam-cons-profile <profile-name>)
2. Associate the ANQP advertisement profile with a Hotspot profile. (wlan hotspot h2-profile advertisement-profile <profile-name>)
3. Enable the hotspot feature within the Hotspot profile. (wlan hotspot h2-profile <profile-name>hotspot-enable)

Parameter	Description
<profile>	Name of an ANQP Roaming Consortium profile.

Examples

The following example shows two ANQP Roaming Consortium profiles configured on the managed device:

```
(host) # show wlan hotspot anqp-roam-cons-profile
ANQP Roaming Consortium Profile List
-----
Name           References  Profile Status
----           -
default        1
Roam_OI2       1
Total:2.
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the ANQP Roaming Consortium profile.
References	Displays the number of other profiles with references to the ANQP Roaming Consortium profile.
Profile Status	Displays whether the ANQP Roaming Consortium profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example displays the configuration settings for the profile **Roam_OI2**:

```
(host) #show wlan hotspot anqp-roam-cons-profile Roam_OI2
ANQP Roaming Consortium Profile "Roam_OI2"
-----
Parameter                Value
-----
Roaming consortium OI Len 3
Roaming consortium OI Len b32af0
```

The output of this command includes the following parameters:

Parameter	Description
Roaming consortium OI Len	Length of the OI. The roaming consortium OI length parameter is based upon the number of octets of the Roaming consortium OI. This parameter can have the following values: <ul style="list-style-type: none"> ▪ 0: 0 Octets in the OI (Null) ▪ 3: OI length is 24-bit (3 Octets) ▪ 5: OI length is 36-bit (5 Octets)
Roaming Consortium OI	The roaming consortium OI sent in a GAS query response.

Related Command

Command	Description
wlan hotspot anqp-roam-cons-profile	This command configures the Roaming Consortium OI information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot anqp-venue-name-profile

```
show wlan hotspot anqp-venue-name-profile [<profile>]
```

Description

The output of this command displays settings for a WLAN ANQP Venue Name profile. ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Use this command without the <profile> parameter to display the entire ANQP Venue Name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Venue Name profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-venue-name-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within the Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile>	Name of an ANQP Venue Name profile.

Examples

The following example shows two ANQP Venue Name profiles configured on the managed device:

```
(host) # show wlan hotspot anqp-venue-name-profile
ANQP Venue Name Profile List
-----
Name           References  Profile Status
----           -
default        0
venue_mall     0
Total:2.
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the ANQP Venue Name profile.
References	Displays the number of other profiles with references to the ANQP Venue Name profile.
Profile Status	Displays whether the ANQP Venue Name profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

This following example shows the configuration settings for the profile **venue_mall**:

```
(host) #show wlan hotspot anqp-venue-name-profile venue_mall
ANQP Venue Name Profile "venue_mall"
-----
Parameter      Value
-----
Venue Group    mercantile
Type of Venue  mercantile-shopping-mall
Venue Name     Westfield_Mall
```

The output of this command includes the following parameters:

Parameter	Description
Venue Group	The venue group to be advertised in the ANQP IEs from APs associated with this profile. This parameter can have any of the following values: <ul style="list-style-type: none"> ▪ assembly ▪ business ▪ educational ▪ factory-or-industrial ▪ institutional ▪ mercantile ▪ outdoor ▪ reserved ▪ residential ▪ storage ▪ unspecified ▪ Utility-Misc ▪ Vehicular

Parameter	Description
Type of Venue	The venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 4155 .
Venue Name	The venue name to be advertised in the ANQP IEs from APs associated with this profile.

Related Command

Command	Description
wlan hotspot anqp-venue-name-profile	This command defines venue information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot h2qp-conn-capability-profile

show wlan hotspot h2qp-conn-capability-profile [<profile>]

Description

The output of this command displays settings for a WLAN H2QP connection capability profile. The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about the IP protocols and associated port numbers that are available and open for communication.

Values configured in this profile will not be sent to clients unless you:

1. Associate the H2QP profile with an ANQP advertisement profile. (wlan hotspot advertisement profile <profile-name> h2qp-conn-cap-profile <profile-name>)
2. Associate the ANQP advertisement profile with a Hotspot profile. (wlan hotspot h2-profile advertisement-profile <profile-name>)
3. Enable the hotspot feature within the Hotspot profile. (wlan hotspot h2-profile <profile-name> hotspot-enable)

Parameter	Description
<profile>	Name of H2QP connection capability profile

Examples

Issue this command without the optional <profile> parameter to display a list of all configured connection capability profiles. Include the <profile> parameter to display details for a specific profile.

The following example shows four H2QP connection capability profiles configured on the managed device:

```
(host) (mynode) show wlan hotspot h2qp-conn-capability-profile
H2QP Connection Capability Profile List
-----
Name           References  Profile Status
----           -
branch-hotspot-1  6
branch-hotspot-2  5
default         1
downtown-hotspot  1
Total:4
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the H2QP connection capability profile.
References	Displays the number of other profiles with references to the H2QP connection capability profile.
Profile Status	Displays whether the H2QP connection capability profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the current configuration settings for the default H2QP connection capability profile:

```
(host) (config) #show wlan hotspot h2qp-conn-capability-profile default
H2QP Connection Capability Profile "default"
-----
Parameter                                     Value
-----
H2QP Connection Capability ICMP port          Disabled
H2QP Connection Capability FTP port(TCP Protocol) Disabled
H2QP Connection Capability SSH port(TCP Protocol) Disabled
H2QP Connection Capability HTTP port(TCP Protocol) Disabled
H2QP Connection Capability TLS VPN port(TCP Protocol) Disabled
H2QP Connection Capability PPTP VPN port(TCP Protocol) Disabled
H2QP Connection Capability VOIP port(TCP Protocol) Disabled
H2QP Connection Capability VOIP port(UDP Protocol) Disabled
H2QP Connection Capability IKEv2 port for IPsec VPN Disabled
H2QP Connection Capability May be used by IKEv2 port for IPsec VPN Disabled
H2QP Connection Capability ESP port(Used by IPsec VPN) Disabled
```

The output of this command includes the following parameters:

Parameter	Description
H2QP Connection Capability ICMP port	Shows if the ICMP port is enabled and available. (port 0)
H2QP Connection Capability FTP port	Shows if the FTP port is enabled and available. (port 20)
H2QP Connection Capability SSH port	Shows if the SSH port is enabled and available. (port 22)
H2QP Connection Capability HTTP port	Shows if the HTTP port is enabled and available. (port 80)
H2QP Connection Capability TLS VPN port	Shows if the TCP TLS port used VPNs is enabled and available. (port 80)

Parameter	Description
H2QP Connection Capability PPTP VPN port	Shows if the PPTP port used by IPsec VPNs is enabled and available. (port 1723)
H2QP Connection Capability VoIP port (UDP)	Shows if the UDP VoIP port is enabled and available. (port 5060)
H2QP Connection Capability VoIP port (TCP)	Shows if the TCP VoIP port is enabled and available. (port 5060)
H2QP Connection Capability IKEv2 port for IPsec VPN	Shows if the IKEv2 port 4500 is enabled and available
H2QP Connection Capability May be used by IKEv2 port for IPsec VPN	Shows if the IKEv2 port 500 is enabled and available
H2QP Connection Capability ESP port (Used by IPsec VPN)	Shows if the ESP port used by IPsec VPNs is enabled and available. (port 0)

Related Command

Command	Description
wlan hotspot h2qp-conn-capability-profile	This command defines an H2QP profile that advertises hotspot protocol and port capabilities.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot h2qp-op-cl-profile

```
show wlan hotspot h2qp-op-cl-profile [<profile>]
```

Description

The output of this command displays settings for a WLAN H2QP operating class profile. The values configured in this H2QP Operating Class profile list the channels on which the hotspot is capable of operating. It may be useful where, for instance, a mobile device discovers a hotspot in the 2.4 GHz band but finds it is dual-band and prefers the 5 GHz band.

Parameter	Description
<profile>	Name of H2QP operating class profile.

Examples

Use this command without the optional <profile> parameter to display a list of all configured connection capability profiles. Include the <profile> parameter to display details for a specific profile.

The following example shows two H2QP operating class profiles configured on the managed device. The **References** column lists the number of other profiles with references to the connection capability profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) (H2QP Connection Capability Profile "default") #show wlan hotspot
h2qp-op-cl-profile
H2QP Operating Class Indication Profile List
-----
Name      References  Profile Status
-----
default   0
newopcl   1
Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the H2QP operating class profile.
References	Displays the number of other profiles with references to the H2QP operating class profile.

Parameter	Description
Profile Status	Displays whether the H2QP operating class profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the current configuration setting for the default H2QP operating class profile:

```
(host) (H2QP Connection Capability Profile "default") #show wlan hotspot
h2qp-op-cl-profile default
H2QP Operating Class Indication Profile "default"
-----
Parameter                               Value
-----
H2QP Operating Class (Valid Values 1-255) 1
```

The output of this command includes the following parameters:

Parameter	Description
H2QP Operating Class (Valid Values 1-255)	Displays the current operating class for the devices BSS. The supported range for this field is 1-255, and the default value is 1.

Related Command

Command	Description
wlan hotspot h2qp-op-cl-profile	Use this command to configure WLAN H2QP operating class profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot h2qp-operator-friendly-name-profile

show wlan hotspot h2qp-operator-friendly-name-profile [<profile>]

Description

The output of this command displays settings for a H2QP operator-friendly name profile. The operator-friendly name defined in this profile is a free-form text field that can identify the operator and also something about the location. Use this command without the <profile> parameter to display the entire operator-friendly name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile>	Name of H2QP operator-friendly name profile.

Examples

The following example shows two H2QP operator-friendly name profiles configured on the managed device:

```
(host)(config)# show wlan hotspot h2qp-operator-friendly-name-profile
H2QP Operator Friendly Name Profile List
-----
Name           References  Profile Status
----           -
default        0
operator1      8
Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the H2QP operator-friendly name profile.
References	Displays the number of other profiles with references to the H2QP operator-friendly name profile.
Profile Status	Displays whether the H2QP operator-friendly name profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the configuration settings for the profile **operator1**:

```
(host) (H2QP Operator Friendly Name Profile "operator1") #show wlan hotspot
h2qp-operator-friendly-name-profile operator1
H2QP Operator Friendly Name Profile "operator1"
-----
Parameter                               Value
-----
Operator Friendly Name Language Code    eng
Operator Friendly Name                   CoffeeHouseGuest
```

The output of this command includes the following parameters:

Parameter	Description
Operator Friendly Name Language Code	An ISO 639 language code that identifies the language used in the Operator Friendly Name field.
Operator Friendly Name	An operator-friendly name sent by devices using this profile. The name can be up to 64 alphanumeric characters, and can include special characters and spaces. If the name includes quotation marks ("), you must include a backslash character (\) before each quotation mark. (e.g. \"example\")

Related Command

Command	Description
ntp	This command defines an H2QP operator-friendly name profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot h2qp-osu-prov-list-profile

```
show wlan hotspot h2qp-osu-prov-list-profile <profile-name>
```

Description

This command displays settings for a H2QP OSU providers list profile. The name defined in this profile is a free-form text field that can identify the OSU providers list. Use this command without the <profile-name> parameter to display the entire OSU providers profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of the H2QP OSU providers list profile.

Example

The following example shows one H2QP OSU providers list profile configured on the managed device:

```
(host) [mynode] ##show wlan hotspot h2qp-osu-prov-list-profile

H2QP OSU Providers List Profile List
-----
Name      References  Profile Status
-----
test-osu  2
Total:1
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the H2QP OSU providers list profile.
References	Displays the number of other profiles with references to the H2QP OSU providers list profile.
Profile Status	Displays whether the H2QP OSU providers list profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

Related Command

Command	Description
<u>wlan hotspot h2qp-wan-metrics-profile</u>	This command creates an H2QP profile that specifies the hotspot WAN status and link metrics.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan hotspot h2qp-wan-metrics-profile

```
show wlan hotspot h2qp-wan-metrics-profile [<profile-name>]
```

Description

The output of this command displays settings for a H2QP WAN metrics profile. The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about access network characteristics such as link status and the capacity and speed of the WAN link to the Internet. Use this command without the `<profile-name>` parameter to display the entire WAN metrics profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><profile-name></code>	Name of H2QP WAN metrics profile.

Examples

The following example shows two H2QP WAN metrics profiles configured on the managed device:

```
(host) [mynode] (H2QP Connection Capability Profile "default") #show wlan
hotspot h2qp-wan-metrics-profile

H2QP WAN Metrics Profile List
-----
Name      References  Profile Status
-----
default   0
fastwan   6
Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the H2QP WAN metrics profile.
References	Displays the number of other profiles with references to the H2QP WAN metrics profile.
Profile Status	Displays whether the H2QP WAN metrics profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the current configuration settings for the profile **fastwan**:

```
(host) [mynode] #show wlan hotspot h2qp-wan-metrics-profile fastwan

H2QP WAN Metrics Profile "fastwan"
-----
Parameter                               Value
-----
H2QP WAN metrics link status            link_up
H2QP WAN metrics symmetric WAN link     Disabled
H2QP WAN metrics link at capacity       Disabled
WAN Metrics uplink speed                 1000
WAN Metrics downlink speed              1000
WAN Metrics uplink load                  100
WAN Metrics downlink load                100
WAN Metrics load measurement duration    100
```

The output of this command includes the following parameters:

Parameter	Description
H2QP WAN metrics link status	Indicates the status of the WAN Link by displaying one of the following values. The default link status is reserved , which indicates that the link status is unknown or unspecified. <ul style="list-style-type: none"> link_down link_test link_up reserved
H2QP WAN metrics symmetric WAN link	This parameter indicates if the WAN Link has same speed in both the uplink and downlink directions.
H2QP WAN metrics link at capacity	This parameter indicates if the WAN Link has reached its maximum capacity. If this parameter is enabled, no additional mobile devices will be permitted to associate to the hotspot AP.
WAN Metrics uplink speed	This parameter indicates the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified.
WAN Metrics downlink speed	This parameter indicates the current WAN backhaul downlink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.
WAN Metrics uplink load	The percentage of the WAN uplink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.

Parameter	Description
WAN Metrics downlink load	The percentage of the WAN downlink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.
WAN Metrics load measurement duration	Duration over which the downlink load is measured, in tenths of a second.

Related Command

Command	Description
wlan hotspot h2qp-wan-metrics-profile	This command creates an H2QP profile that specifies the hotspot WAN status and link metrics.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

show wlan hotspot hs2-profile

```
show wlan hotspot hs2-profile [<profile-name>]
```

Description

The output of this command displays settings for a Hotspot 2.0 profile. Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority. The Roaming Consortium IEs contain information identifying the network and service provider, whose security credentials can then be used to authenticate with the AP transmitting this element.

The OI for the service provider is defined in the ANQP Roaming Consortium profile using the [wlan hotspot anqp-roam-cons-profile](#) command. This Hotspot profile allows you to define and send up to three additional OIs to a client. The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Use this command without the `<profile-name>` parameter to display the entire ANQP advertisement profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><profile-name></code>	Name of a Hotspot 2.0 profile.

Examples

The following example shows two Hotspot profiles configured on the managed device:

```
(host) [mynode] # show wlan hotspot hs2-profile

Hotspot 2.0 Profile List
-----
Name           References  Profile Status
----           -
default        1
Hotspot_1      2
Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the Hotspot 2.0 profile.

Parameter	Description
References	Displays the number of other profiles with references to the Hotspot 2.0 profile.
Profile Status	Displays whether the Hotspot 2.0 profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows configuration settings defined for the profile **Hotspot1**:

```
(host) [mynode] #show wlan hotspot hs2-profile Hotspot1

Hotspot 2.0 Profile "default"
-----
Parameter
Value
-----
-
Advertise Hotspot 2.0 Capability
Enabled
Additional Steps required for Access Enabled
Enabled
Network Internet Access
Enabled
Length of Query Response
octets
255
Access network Type
public-chargeable
Roaming Consortium Len Entry 1
octets
3
Roaming Consortium OI Entry 1
C499AA
Roaming Consortium Len Entry 2
0
Roaming Consortium OI Entry 2
N/A
Roaming Consortium Len Entry 3
0
Roaming Consortium OI Entry 3
N/A
Additional Roaming Consortium OI's (displayed in Advertisement Profile)
1
Venue Group Type
mercantile
Venue Type
mercantile-shopping-mall
Type of Hotspot 2.0 Indication Element
31
Advertisement Profile
Westgate_Mall
```

The output of this command includes the following parameters:

Parameter	Description
Advertise Hotspot 2.0 Capability	Shows if this profile has been enabled.
Additional Steps required for Access Enabled	<p>If this parameter is enabled, the AP will send the following IEs (IEs) in response to the client's the ANQP query.</p> <ul style="list-style-type: none"> ▪ Venue Name ▪ Domain Name List ▪ Network Authentication Type ▪ Roaming Consortium List ▪ NAI Realm List <p>NOTE: If asra is enabled, the advertisement profile for this hotspot must reference an enabled network authentication type profile. For more information on enabling an network authentication type profile, see wlan hotspot anqp-nwk-auth-profile on page 4150.</p>
Network Internet Access	If enabled, the AP sends an Information Element (IE) indicating that the network allows internet access. By default, a hotspot profile does not advertise network internet access.
Length of Query Response	The maximum length of the GAS query response, in octets. The supported range is 1-255 octets.
Access network Type	<p>The 802.11u network type. The default setting is public-chargeable.</p> <ul style="list-style-type: none"> ▪ emergency-services: emergency services only network ▪ personal-device: personal device network ▪ private: private network ▪ private-guest: private network with guest access ▪ public-chargeable: public chargeable network ▪ public-free: free public network ▪ test: test network ▪ wildcard: wildcard network
Roaming Consortium Len Entry 1	<p>Length of the OI. This value is based upon the number of octets in the Roaming Consortium OI Entry 1 field.</p> <ul style="list-style-type: none"> ▪ 0: Zero Octets in the OI (Null) ▪ 3: OI length is 24-bit (3 Octets) ▪ 5: OI length is 36-bit (5 Octets)

Parameter	Description
Roaming Consortium OI Entry 1	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the Additional Roaming Consortium OI's (displayed in Advertisement Profile) parameter is set to 1 or higher.
Roaming Consortium Len Entry 2	Length of the OI. This value is based upon the number of octets in the Roaming Consortium OI Entry 2 field. <ul style="list-style-type: none"> ▪ 0: Zero Octets in the OI (Null) ▪ 3: OI length is 24-bit (3 Octets) ▪ 5: OI length is 36-bit (5 Octets)
Roaming Consortium OI Entry 2	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the Additional Roaming Consortium OI's (displayed in Advertisement Profile) parameter is set to 2 or higher.
Roaming Consortium Len Entry 3	Length of the OI. This value is based upon the number of octets in the Roaming Consortium OI Entry 3 field. <ul style="list-style-type: none"> ▪ 0: Zero Octets in the OI (Null) ▪ 3: OI length is 24-bit (3 Octets) ▪ 5: OI length is 36-bit (5 Octets)
Roaming Consortium OI Entry 3	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the Additional Roaming Consortium OI's (displayed in Advertisement Profile) parameter is set to 3 or higher.
Additional Roaming Consortium OI's (displayed in Advertisement Profile)	Number of additional roaming consortium Organization Identifiers (OIs) advertised by the AP.
Venue Group Type	The venue groups to be advertised in the IEs from APs associated with this hotspot profile. The default setting is unspecified .
Venue Type	Venue type to be advertised in the IEs from APs associated with this hotspot profile.
Type of Hotspot 2.0 Indication Element	Advertisement protocol types to be used by the AP. <ul style="list-style-type: none"> ▪ anqp: Access Network Query Protocol ▪ emergency: Emergency Alert System

Parameter	Description
	<ul style="list-style-type: none"> ▪ mih-cmd-event: Media Independent Handover (MIH) Command and Event Services Capability Discovery ▪ mih-info: Media Independent Handover (MIH) Information Service. This option allows handovers between differing kinds of wireless access protocols and technologies, allowing access points on different IP subnets to communicate with each other at the link level while maintaining session continuity.
Advertisement Profile	Advertisement profile associated with this hotspot profile.

Related Command

Command	Description
wlan hotspot hs2-profile	This command configures a hotspot profile for an 802.11u public access service provider.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan ht-ssid-profile

```
show wlan ht-ssid-profile [<profile-name>]
```

Description

This command displays the list of all high-throughput SSID profiles, or detailed configuration information for a specific high-throughput SSID profile. Use this command without the `<profile-name>` parameter to display the entire high-throughput SSID profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><profile-name></code>	Name of a high-throughput SSID profile.

Examples

The following example shows three high-throughput SSID profiles configured on the managed device:

```
(host) [mynode] #show wlan ht-ssid-profile

High-throughput SSID profile List
-----
Name                               References  Profile Status
----                               -
default                             2
dot1X_CP-htssid_prof                1
ade-sloan-htssid_prof               1

Total:3
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the high-throughput SSID profile.
References	Displays the number of other profiles with references to the high-throughput SSID profile.
Profile Status	Displays whether the high-throughput SSID profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows configuration settings defined for the profile **default**:

```
(host) #show wlan ht-ssid-profile default

High-throughput SSID profile "default"
-----
Parameter                                     Value
-----
High throughput enable (SSID)                 Enabled
40 MHz channel usage                         Enabled
Very High throughput enable (SSID)           Enabled
80 MHz channel usage (VHT)                   Enabled
BA AMSDU Enable                              Enabled
Temporal Diversity Enable                    Disabled
Legacy stations                              Allowed
Low-density Parity Check                     Enabled
Maximum number of spatial streams usable for STBC reception 1
Maximum number of spatial streams usable for STBC transmission 1
MPDU Aggregation                             Enabled
Max received A-MPDU size                     65535 bytes
Max transmitted A-MPDU size                  65535 bytes
Min MPDU start spacing                       0 usec
Short guard interval in 20 MHz mode           Enabled
Short guard interval in 40 MHz mode           Enabled
Short guard interval in 80 MHz mode           Enabled
Supported MCS set                            0-31
VHT - Supported MCS map                      9,9,9,9
VHT - Explicit Transmit Beamforming           Enabled
VHT - Transmit Beamforming Sounding Interval 25 msec
VHT - Multi User Transmit Beamforming         Enabled
Maximum VHT MPDU size                        11454 bytes
Maximum number of MSDUs in an A-MSDU on best-effort AC 2 MSDUs
Maximum number of MSDUs in an A-MSDU on background AC 2 MSDUs
Maximum number of MSDUs in an A-MSDU on video AC 2 MSDUs
Maximum number of MSDUs in an A-MSDU on voice AC 0 MSDUs
```

The output of this command includes the following parameters:

Parameter	Description
High throughput enable (SSID)	Displays if the high-throughput (802.11n) feature is enabled or disabled on the SSID. Default: Enabled.
40 MHz channel usage	Shows if the profile enables or disables the use of 40 MHz channels. Default: Enabled.
Very High throughput enable (SSID)	Displays if the very high-throughput (802.11ac) feature is enabled or disabled on the SSID. Default: Enabled.
80 MHz channel usage (VHT)	Displays the status of the 80 MHz channel for very high-throughput is enabled or disabled.

Parameter	Description
	Default: Enabled.
BA AMSDU Enable	Displays if the AP has enabled or disabled the ability to receive Aggregated-MAC Service Data Unit (A-MSDU) in Block ACK (BA) negotiation. Default: Enabled.
Temporal Diversity Enable	Displays if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries. Default: Disabled.
Legacy stations	Allows or disallows associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
Low-density Parity Check	If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise. Default: Enabled.
Maximum number of spatial streams usable for STBC reception	Displays the maximum number of spatial streams usable for Space-Time Block Code (STBC) reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) NOTE: If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
Maximum number of spatial streams usable for STBC transmission	Displays the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) NOTE: If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
MPDU Aggregation	Displays if the profile enables or disables MAC Protocol Data Unit (MPDU) aggregation. Default: Enabled.

Parameter	Description
Max received A-MPDU size	Displays the configured maximum size of a received aggregate MPDU, in bytes.
Max transmitted A-MPDU size	Displays the configured maximum size of a transmitted aggregate MPDU, in bytes.
Min MPDU start spacing	Displays the configured minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
Short guard interval in 20 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 20 MHz mode. Default: Enabled.
Short guard interval in 40 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 40 MHz mode. Default: Enabled.
Short guard interval in 80 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 80 MHz mode. Default: Enabled.
Supported MCS set	<p>Displays a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz vs. 80 MHz) and the number of spatial streams used by the mesh node.</p> <p>Default: 0-31</p> <ul style="list-style-type: none"> ▪ MCS value of 16-23 are supported on 130 Series, RAP-155, and 11ac APs only. ▪ MCS value of 24-31 are supported on 320 Series APs only.
VHT - Supported MCS map	<p>Displays a list of supported MCS map for very high throughput SSID. Comma separated list of maximum supported MCS for spatial streams 1 through 4. Valid values for maximum MCS are 7, 8, 9, and '-' (if spatial stream is not supported). Maximum MCS of a spatial stream cannot be higher than the previous streams. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx.</p> <p>Default: 9,9,9,9.</p>

Parameter	Description
VHT - Explicit Transmit Beamforming	<p>Displays if VHT Explicit Transmit Beamforming status is enabled or disabled for the 802.11ac-capable APs. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this parameter is disabled, all other transmit beamforming settings will not take effect. Default: Enabled.</p>
VHT - Transmit Beamforming Sounding Interval	<p>Displays the time interval in milliseconds between updates of VHT Transmit Beamforming channel estimation. (802.11ac-capable APs only)</p> <p>NOTE: This is applicable for 802.11ac-capable APs only.</p> <p>Default: 25 milliseconds.</p>
VHT - Multi User Transmit Beamforming	<p>Displays if the VHT Multi-User Transmit Beamforming is enabled or disabled. If this parameter is disabled, all other Multi-User Transmit Beamforming configuration parameters have no effect.</p> <p>NOTE: This parameter is applicable for 320 Series APs only.</p> <p>Default: Enabled.</p>
Maximum VHT MPDU size	<p>Displays the maximum size of a VHT MPDU. Default: 11454 bytes.</p>
Maximum number of MSDUs in an A-MSDU on best-effort AC	<p>Displays the maximum number of MSDUs in a TX A-MSDU on best-effort Access Category (AC). Default: 2.</p> <p>NOTE: In tunnel and decrypt-tunnel forwarding mode, TX A-MSDU is disabled if the value is set to 0. If the value is set to non-zero, TX A-MSDU is enabled and set to this value.</p>
Maximum number of MSDUs in an A-MSDU on background AC	<p>Displays the maximum number of MSDUs in a TX A-MSDU on background AC. Default: 2.</p> <p>NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on background AC is disabled and</p>

Parameter	Description
	assigning any value has no effect.
Maximum number of MSDUs in an A-MSDU on video AC	Displays the maximum number of MSDUs in a TX A-MSDU on video AC. Default: 2. NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on video AC is disabled and assigning any value has no effect.
Maximum number of MSDUs in an A-MSDU on voice AC	Displays the maximum number of MSDUs in a TX A-MSDU on voice AC. Default: 0. NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on voice AC is disabled and assigning any value has no effect.

Related Command

Command	Description
wlan ht-ssid-profile	This command configures a high-throughput SSID profile.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan mu-edca-parameters-profile

```
show wlan mu-edca-parameters-profile <profile-name>
```

Description

This command displays the MU EDCA Parameters profiles. The optional output modifiers begin , exclude, and include help you display those lines that begin, include, and exclude respectively, the line expression given in the CLI command. The redirect-output modifier helps you redirect the command output.

Parameter	Description
<profile-name>	Name of the MU EDCA parameter profile.

Example

The following example shows an MU EDCA Parameters profile configured on the managed device:

```
(host)[mynode] #show wlan mu-edca-parameters-profile
MU EDCA Parameters profile List
-----
Name      References  Profile Status
-----
default  1
Total:1
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the MU EDCA Parameters profile.
References	Displays the number of other profiles with references to the MU EDCA Parameters profile.
Profile Status	Displays whether the MU EDCA Parameters profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan rrm-ie-profile

```
show wlan rrm-ie-profile [<profile-name>]
```

Description

This command displays the list of all radio resource management information element (RRM IE) profiles, or the detailed configuration information for a specific RRM IE profile. Use this command without the <profile-name> parameter to display the entire RRM IE profile list. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of an RRM IE profile.

Examples

The following example shows an RRM IE profile configured on the managed device:

```
(host) [mynode] #show wlan rrm-ie-profile

RRM IE Profile List
-----
Name                               References  Profile Status
----                               -
test-rrm-profile                   1
Total:1
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the RRM IE profile.
References	Displays the number of other profiles with references to the RRM IE profile.
Profile Status	Displays whether the RRM IE profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the configuration information for the **default** RRM IE profile:

```
(host) [mynode] #show wlan rrm-ie-profile default

RRM IE Profile "default"
-----
Parameter                               Value      Set
-----
Advertise Enabled Capabilities IE      Enabled
Advertise Country IE                   Enabled
Advertise Power Constraint IE          Enabled
Advertise TPC Report IE                Enabled
Advertise QBSS Load IE                 Enabled
Advertise BSS AAC IE                   Enabled
Advertise Quiet IE                     Enabled
```

Related Command

Command	Description
wlan rrm-ie-profile	This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan sae-profile

```
show wlan sae-profile
```

Description

This command displays the WPA3 Simultaneous Authentication of Equals (SAE) profiles. The optional output modifiers `begin`, `exclude`, and `include` help you display those lines that begin, include, and exclude respectively, the line expression given in the CLI command. The `redirect-output` modifier helps you redirect the command output.

Example

The following example shows an SAE profile configured on the managed device:

```
(host)[mynode] #show wlan sae-profile
WPA3 SAE Configuration
-----
Parameter                               Value
-----
Auth Frame Retransmit Interval <20-1000>ms 100
SAE Anti-Clogging token threshold <0-1000> 5
SAE Giveup threshold <1-20>                5
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan ssid-profile

```
show wlan ssid-profile [<profile-name>]
```

Description

This command displays the list of all SSID profiles, or detailed configuration information for a specific SSID profile. Use this command without the `<profile-name>` parameter to display the entire SSID profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><profile-name></code>	Name of an SSID profile.

Examples

The following example shows six SSID profiles configured on the managed device:

```
(host) [mynode] #show wlan ssid-profile

SSID Profile List
-----
Name                               References  Profile Status
----                               -
coltrane-ssid-profile              1
corp1 -ssid-profile                3
Remote                             1
Secure-Profile2                   0
test-ssid-profile                  1
wizardtest-ssid-profile            1

Total:6
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the SSID profile.
References	Displays the number of other profiles with references to the SSID profile.
Profile Status	Displays whether the SSID profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows configuration settings defined for the SSID Profile **Remote**:

```
(host) [mynode] #show wlan ssid-profile remote

SSID Profile "Remote"
-----
Parameter                               Value
-----
SSID enable                             Enabled
ESSID                                    aruba-ap
Encryption                               opensystem
Enable Management Frame Protection       Disabled
Require Management Frame Protection      Disabled
DTIM Interval                            1 beacon periods
802.11a Basic Rates                      6 12 24
802.11a Transmit Rates                   6 9 12 18 24 36 48 54
802.11g Basic Rates                      1 2
802.11g Transmit Rates                   1 2 5 6 9 11 12 18 24 36
48 54
Station Ageout Time                      1000 sec
Station Refresh Direction                 bidirectional
Max Transmit Attempts                     8
RTS Threshold                             2333 bytes
Short Preamble                            Enabled
Max Associations                           64
Wireless Multimedia (WMM)                Disabled
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave Enabled
WMM TSPEC Min Inactivity Interval         0 msec
WMM DSCP Mapping Control                  Enabled
DSCP mapping for WMM voice AC              N/A
DSCP mapping for WMM video AC              N/A
DSCP mapping for WMM best-effort AC        N/A
DSCP mapping for WMM background AC         N/A
Multiple Tx Replay Counters                Disabled
Hide SSID                                 Disabled
Deny_Broadcast Probes                     Disabled
Local Probe Request Threshold (dB)         0
Auth Request Threshold (dB)                0
Disable Probe Retry                       Enabled
Battery Boost                              Disabled
WEP Key 1                                 N/A
WEP Key 2                                 N/A
WEP Key 3                                 N/A
WEP Key 4                                 N/A
WEP Transmit Key Index                     1
WPA Hexkey                                 N/A
WPA Passphrase                             N/A
Maximum Transmit Failures                  0
EDCA Parameters Station profile            N/A
EDCA Parameters AP profile                 N/A
BC/MC Rate Optimization                    Disabled
Rate Optimization for delivering EAPOL frames Enabled
Strict Spectralink Voice Protocol (SVP)    Disabled
High-throughput SSID Profile               default
802.11g Beacon Rate                       default
802.11a Beacon Rate                       default
```

```

Video Multicast Rate Optimization      default
Advertise QBSS Load IE                Disabled
Advertise Location Info               Enabled
Advertise AP Name                     Disabled
802.11r Profile                       N/A
Enforce user vlan for open stations   Enabled
Enable OKC                            Enabled

```

The output of this command includes the following parameters:

Parameter	Description
SSID	Shows if the profile has enabled or disabled this SSID.
ESSID	Name that uniquely identifies a wireless network. If the ESSID includes spaces, you must enclose it in quotation marks.
Encryption	The layer-2 authentication and encryption type used on this ESSID.
Enable Management Frame Protection	Enables management frame protection.
Require Management Frame Protection	If enabled, requires management frame protection.
DTIM Interval	The interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon.
802.11a Basic Rates	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11a Transmit Rates	Set of 802.11a rates at which the AP is allowed to send data.
802.11g Basic Rates	List of supported 802.11b/g rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11g Transmit Rates	Set of 802.11b/g rates at which the AP is allowed to send data.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Station Refresh Direction	The refresh direction of WLAN SSID profile.
Max Transmit Attempts	Maximum transmission failures allowed before the client gives up.

Parameter	Description
RTS Threshold	Wireless clients transmitting frames larger than this defined threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS).
Short Preamble	Shows if the profile enables or disables short preamble for 802.11b/g radios
Max Associations	Maximum number of wireless clients for the AP
Wireless Multimedia (WMM)	Shows if the profile enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF)
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	Shows if the profile enables or disables Wireless Multimedia (WMM) UAPSD powersave.
WMM TSPEC Min Inactivity Interval	Specifies the minimum inactivity time-out threshold of WMM traffic.
DSCP mapping for WMM voice AC	DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	DSCP value used to map WMM best-effort traffic.
DSCP mapping for WMM background AC	DSCP value used to map WMM background traffic.
902iL Compatibility Mode	(For clients using NTT DoCoMo 902iL phones only) When enabled, the managed device does not drop packets from the client if a small or old initialization vector value is received.
Hide SSID	Shows if the profile enables or disables hiding of the SSID name in beacon frames.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if the profile enables or disables local probe response on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the managed device sends the 802.11 probe responses.

Parameter	Description
Auth Request Threshold (dB)	Displays the SNR threshold below which incoming authentication requests are ignored.
Disable Probe Retry	Shows if the profile enables or disables battery MAC level retries for probe response frames.
Battery Boost	If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval.
WEP Key 1	Displays the Static WEP key associated with this key index.
WEP Key 2	Displays the Static WEP key associated with this key index.
WEP Key 3	Displays the Static WEP key associated with this key index.
WEP Key 4	Displays the Static WEP key associated with this key index.
WEP Transmit Key Index	Shows the key index that specifies which static WEP key is to be used.
WPA Hexkey	WPA pre-shared key (PSK).
WPA Passphrase	WPA passphrase used to generate a pre-shared key (PSK).
Maximum Transmit Failures	Maximum transmission failures allowed before the client gives up.
EDCA Parameters Station profile	Name of the enhanced distributed channel access (EDCA) Station profile that applies to this SSID.
EDCA Parameters AP profile	Name of the enhanced distributed channel access (EDCA) AP profile that applies to this SSID.
BC/MC Rate Optimization	Shows if the profile enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
Rate Optimization for delivering EAPOL frames	If this option is enabled, APs using this profile will use a more conservative rate for more reliable delivery of EAPOL frames.
Strict Spectralink Voice Protocol (SVP)	Shows if the profile enables or disables strict Spectralink Voice Protocol (SVP).

Parameter	Description
High-throughput SSID Profile	Name of the high-throughput SSID profile associated with this SSID profile.
802.11g Beacon Rate	The beacon rate for 802.11g (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.
802.11a Beacon Rate	The beacon rate for 802.11a (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.
Video Multicast Rate Optimization	The rate for video multicast frames.
Advertise QBSS Load IE	<p>Enables the AP to advertise the QBSS load element. The element includes the following parameters that provide information on the traffic situation:</p> <ul style="list-style-type: none"> ▪ Station count: The total number of stations associated to the QBSS. ▪ Channel utilization: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel. ▪ Available admission capacity: The remaining amount of medium time (measured as number of 32us/s) available for a station via explicit admission control. <p>The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points.</p>
Advertise Location Info	APs that are part of this VAP will broadcast their GPS coordinates in the beacons and probe response frames as part of a vendor-specific Information Element.
Advertise AP Name	If this parameter enabled, APs will broadcast the AP name configured by the ap-name command. This option is disabled by default.
802.11r Profile	The associated dot11r-profile with the SSID profile.
Enforce user vlan for open stations	Shows the strict enforcement of data traffic only in user's assigned vlan (Open stations only).
Enable OKC	The status of the Opportunistic Key Caching.

Parameter	Description
	Opportunistic Key Caching (OKC) is a similar technique, not defined by 802.11i, available for authentication between multiple APs in a network where those APs are under common administrative control. An Aruba deployment with multiple APs under the control of a single controller is one such example. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

Related Command

Command	Description
wlan ssid-profile	This command configures an SSID profile.

Command History

Release	Modification
ArubaOS 8.5.0.0	The <code>Station Refresh Direction</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan traffic-management-profile

show wlan traffic-management-profile [<profile-name>]

Description

This command displays the list of all traffic management profiles, or detailed configuration information for a specific traffic management profile. Issue this command without the <profile-name> parameter to display the entire traffic management profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of a traffic management profile.

Examples

The following example shows two traffic management profiles configured on the managed device:

```
(host) [mynode] #show wlan traffic-management-profile

Traffic management profile List
-----
Name           References  Profile Status
-----
mgmt1          3
mgmt2          2
Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the traffic management profile.
References	Displays the number of other profiles with references to the traffic management profile.
Profile Status	Displays whether the traffic management profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows configuration settings defined for the profile **mgmt1**:

```
(host) [mynode] #show wlan traffic-management-profile mgmt1

Traffic management profile "default"
-----
Parameter                Value
-----
Proportional BW Allocation N/A
Report interval           5 min
Station Shaping Policy    default-access
```

The output of this command includes the following parameters:

Parameter	Description
Proportional BW Allocation	Minimum bandwidth, as a percentage of available bandwidth, allocated to an SSID when there is congestion on the wireless network. An SSID can use all available bandwidth if no other SSIDs are active.
Report interval	Number of minutes between bandwidth usage reports.
Station Shaping Policy	Shows which of three possible Station Shaping policies is configured on the profile. <ul style="list-style-type: none">▪ default-access: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting.▪ fair-access: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The bw-alloc parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP.▪ preferred-access: High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.

Related Command

Command	Description
wlan traffic-management-profile	This command configures a traffic management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wlan tsm-req-profile

```
show wlan tsm-req-profile [<profile-name>]
```

Description

This command displays configuration and other information about the parameters for the Transmit Stream and Category Measurement (TSM) Request frames. Issue this command without the <profile-name> parameter to display the entire TSM Request profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

For this profile to take effect, the 802.11K feature needs to be enabled.

Parameter	Description
<profile-name>	Name of a TSM Report Request profile. The name must be between 1-63 characters.

Example

The following example shows the parameters description of a TSM Report Request profile:

```
(host) [mynode] #show wlan tsm-req-profile default

TSM Report Request Profile "default"
-----
Parameter                               Value
-----
Request Mode for TSM Report Request      normal
Number of repetitions                     65535
Duration Mandatory                       Enabled
Randomization Interval                   0
Measurement Duration                      25
Traffic ID                               96
Bin 0 Range                              200
```

The output of this command includes the following parameters:

Parameter	Description
Request mode for TSM Report Request	Shows the request mode for the Transmit Stream and Category Measurement Request frame.
Number of repetitions	Shows the "Number of Repetitions" field in the Transmit Stream and Category Measurement Request frame.

Parameter	Description
Duration Mandatory	Shows the "Duration Mandatory" part of the Measurement Request Mode field of the Transmit Stream and Category Measurement Request frame.
Randomization Interval	Shows the Randomization Interval field in the Transmit Stream and Category Measurement Request frame.
Measurement Duration	Shows the Measurement Duration field in the Transmit Stream and Category Measurement Request frame.
Traffic ID	Shows the Traffic Identifier field in the Transmit Stream and Category Measurement Request frame.
Bin 0 Range	Shows the ' Bin 0 Range ' field in the Transmit Stream and Category Measurement Request frame.

Related Command

Command	Description
wlan tsm-req-profile	This command configures a TSM Report Request Profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan virtual-ap

show wlan virtual-ap [<profile-name>]

Description

Displays the list of all virtual AP profiles, or detailed configuration information for a specific virtual AP profile. Issue this command without the <profile-name> parameter to display the entire virtual AP profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<profile-name>	Name of a virtual AP profile.

Examples

The following example shows six virtual AP profiles configured on the managed device.

```
(host) [mynode] #show wlan virtual-ap

Virtual AP profile List
-----
Name                               References  Profile Status
----                               -
coltrane-vap-profile                1
default
MegTest
Remote                               1
test-vap-profile                    1
wizardtest-vap-profile              1
Total: 6
```

The output of this command includes the following parameters.

Parameter	Description
Name	Displays the name of the virtual AP profile.
References	Displays the number of other profiles with references to the virtual AP profile.
Profile Status	Displays whether the virtual AP profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows the configuration settings defined for the profile **wizardtest-vap-profile**.

```
(host) [mynode] #show wlan virtual-ap test-vap-profile

Virtual AP profile "wizardtest-vap-profile"
-----
Parameter                               Value
-----
AAA Profile                               default
802.11K Profile                           default
SSID Profile                              default
Virtual AP enable                         Enabled
VLAN                                       N/A
Forward mode                             tunnel
Allowed band                             all
Allowed 5 GHz radio                       all
Allow 6GHz band                           Disabled
Disable 6GHz vap for mesh                 Disabled
Band Steering                             Disabled
Fine Timing Measurement (802.11mc Responder Mode Steering Mode) Disabled
Dynamic Multicast Optimization (DMO)      Enabled
Dynamic Multicast Optimization (DMO)      Threshold 6
Drop Broadcast and Multicast               Disabled
Convert Broadcast ARP requests to unicast Enabled
Authentication Failure Blacklist/Denylist Time 3600 sec
Blacklist/Denylist Time                   3600 sec
Deny inter user traffic                   Disabled
Deny time range                           N/A
DoS Prevention                             Disabled
HA Discovery on-association                Disabled
Mobile IP                                  Enabled
Preserve Client VLAN                       Disabled
Remote-AP Operation                       standard
Station Blacklisting/Denylisting          Enabled
Strict Compliance                         Disabled
VLAN Mobility                              Disabled
FDB Update on Assoc                       Disabled
WMM Traffic Management Profile             N/A
Anyspot Profile                           N/A
```

The output of this command includes the following parameters.

Parameter	Description
AAA Profile	Name of the AAA profile associated with this virtual AP.
802.11K Profile	Name of an 802.11k profile associated with this virtual AP.

Parameter	Description
SSID Profile	Name of an SSID profile associated with this virtual AP.
Virtual AP enable	Shows if the profile enables or disables the virtual AP.
VLAN	The VLAN(s) into which users are placed in order to obtain an IP address.
Forward mode	<p>Forwarding mode defined on the profile:</p> <ul style="list-style-type: none"> ▪ tunnel mode ▪ bridge mode ▪ split-tunnel mode ▪ decrypt-tunnel mode <p>The forwarding mode controls whether data is tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local).</p> <p>When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the managed device, which then applies firewall policies to the user traffic. When the managed device sends traffic to a client, the managed device sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client.</p>
Allowed band	<p>The band(s) on which to use the virtual AP:</p> <ul style="list-style-type: none"> ▪ a—802.11a band only (5 GHz) ▪ g—802.11b/g band only (2.4 GHz) ▪ all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)

Parameter	Description
Allowed 5G radio	<p>The 5 GHz radio(s) on which to configure the virtual AP:</p> <ul style="list-style-type: none"> ■ all—dual 5 GHz band only ■ first-5g-radio-only—first 5 GHz band only ■ second-5g-radio-only—second 5 GHz band only <p>NOTE: This parameter is ignored if the AP has only one 5 GHz radio.</p>
Allow 6GHz band	<p>Disable or enable 6 GHz band to use the virtual AP.</p> <p>NOTE: This parameter is applicable to Wi-Fi 6E APs only.</p>
Disable 6GHz vap for mesh	<p>Disable or enable virtual AP on 6 GHz band. If enabled, virtual AP is disabled on 6 GHz band only when AP is provisioned as mesh.</p> <p>NOTE: This parameter is applicable to Wi-Fi 6E APs only.</p>
Band Steering	<p>If enabled, ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones.</p>
Fine Timing Measurement (802.11mc) Responder Mode	<p>Shows if 802.11 mc Fine Timing Measurement (FTM) on radio (responder mode) is enabled for 500 Series, 500H Series, 510 Series, 530 Series, 550 Series, 560 Series, 570 Series, 630 Series, and 650 Series access points.</p>
Steering Mode	<p>Band steering supports three different band steering modes:</p> <ul style="list-style-type: none"> ■ Force-5GHz: When the AP is configured in force-5GHz band steering mode, the AP will try to force 5 Ghz-capable APs to use that radio band.

Parameter	Description
	<ul style="list-style-type: none"> ▪ Prefer-5GHz (Default): If you configure the AP to use prefer-5GHz band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. ▪ Balance-bands: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz while the 2.5 GHz band operates in 20 MHz. <p>NOTE: Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default prefer-5GHz steering mode available in ArubaOS 6.0 and later.</p>
Dynamic Multicast Optimization (DMO)	If enabled DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.

Parameter	Description
Drop Broadcast and Multicast	If enabled, the virtual AP will filter out broadcast and multicast traffic in the air.
Convert Broadcast ARP requests to unicast	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client.
Authentication Failure Blacklist/Denylist Time	Time, in seconds, a client is blocked if it fails repeated authentication. An authentication failure blacklist/denylisttime of 0 blocks failed users indefinitely.
Blacklist/Denylist Time	Number of seconds that a client is quarantined from the network after being blacklisted/denylisted.
Deny Inter User Traffic	<p>This option, when enabled, denies traffic between the clients using this virtual AP profile.</p> <p>The <code>firewall</code> command includes an option to deny all inter-user traffic, regardless of the Virtual AP profile used by those clients.</p> <p>If the global setting to deny inter-user traffic is enabled, all inter-user traffic between clients will be denied, regardless of the settings configured in the virtual AP profiles. If the setting to deny inter-user traffic is disabled globally but enabled on an individual virtual ap, only the traffic between un-trusted users and the clients on that particular virtual AP will be blocked.</p>
Deny time range	Time range for which the AP will deny access.
DoS Prevention	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.

Parameter	Description
HA Discovery on-association	<p>If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practices is to leave this parameter disabled as it increases IP mobility control traffic between controllers in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients.</p> <p>NOTE: <code>ha-disc-onassoc</code> parameter works only when IP mobility is enabled and configured on the controller.</p>
Mobile IP	Shows if the profile has enabled or disabled IP mobility.
Preserve Client VLAN	This parameter allows clients to retain their previous VLAN assignment if the client disassociates from an AP and then immediately re-associates either with same AP or another AP on same controller.
Remote-AP Operation	<p>Shows when the virtual AP operates on a remote AP:</p> <ul style="list-style-type: none"> ▪ always—Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ▪ backup—Enables the virtual AP if the remote AP cannot connect to the controller (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ▪ persistent—Permanently enables the virtual AP after

Parameter	Description
	<p>the remote AP initially connects to the controller (Bridge Mode only). This option can be used for any (Open/PSK/802.1X) bridge VAPs.</p> <ul style="list-style-type: none"> ▪ standard—Enables the virtual AP when the remote AP connects to the controller. This option can be used for any (bridge/split-tunnel/tunnel/d-tunnel) VAPs.
Station Blacklisting/Denylisting	Shows if the profile has enabled or disabled detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed death attacks.
Strict Compliance	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
Multi Association	If enabled, this feature allows a station to be associated to multiple APs. If this feature is disabled, when a station moves to new AP it will be de authorized by the AP to which it was previously connected, deleting station context and flushing key caching information
Fast Roaming	Shows if the AP has enabled or disabled fast roaming.
VLAN Mobility	Shows if the AP has enabled or disabled VLAN (Layer-2) mobility.

Parameter	Description
WMM Traffic Management Profile	WMM Traffic Management Profile associated with this Virtual AP Profile
Anyspot profile	Anyspot Profile associated with this Virtual AP Profile

Related Command

Command	Description
wlan virtual-ap	This command configures a virtual AP profile.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of blacklist have been replaced with whitelist .
ArubaOS 8.8.0.0	The output parameter Fine Timing Measurement (802.11mc) Responder Mode was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wlan wmm-traffic-management-profile

show wlan wmm-traffic-management-profile [<profile-name>]

Description

Displays the list of all WMM traffic management profiles, or detailed configuration information for a specific WMM traffic management profile. Issue this command without the <profile-name> parameter to display the entire WMM traffic management profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
profile-name>	Name of the WMM traffic management profile.

Examples

The following example shows two WMM traffic management profiles configured on the managed device:

```
(host) [mynode] #show wlan wmm-traffic-management-profile

WMM Traffic management profile List
-----
Name          References  Profile Status
-----
default       3
test          2

Total:2
```

The output of this command includes the following parameters:

Parameter	Description
Name	Displays the name of the WMM traffic management profile.
References	Displays the number of other profiles with references to the WMM traffic management profile.
Profile Status	Displays whether the WMM traffic management profile is predefined. NOTE: User-defined profiles do not have an entry in the Profile Status column.

The following example shows configuration settings defined for the profile **test**:

```
(host) [mynode] #show wlan traffic-management-profile test

WMM Traffic management profile "test"
-----
Parameter          Value
-----
Enable Shaping Policy true
Voice Share         40 %
Video Share         43 %
Best-effort Share   10 %
Background Share    7 %
```

The output of this command includes the following parameters:

Parameter	Description
Enable Shaping Policy	Displays if WMM based traffic shaping is enabled on the managed device.
Voice Share	Displays the bandwidth allocation in percentage (%) for voice access traffic category.
Viceo Share	Displays the bandwidth allocation in percentage (%) for video access traffic category.
Best-effort Share	Displays the bandwidth allocation in percentage (%) for best effort access traffic category.
Background Share	Displays the bandwidth allocation in percentage (%) for background access traffic category.

Related Command

Command	Description
wlan wmm-traffic-management-profile	Configures WMM traffic management profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wmm tspec-statistics

```
show wmm tspec-statistics
```

Description

This command displays TSPEC statistics information. A WMM client can send a Traffic Specification (TSPEC) signaling request to the AP before sending traffic of a specific AC type, such as voice.

Example

The output of this command displays TSPEC statistics information.

```
(host) [mynode] #show wmm tspec-statistics

TSPEC Enforcement statistics
-----
Name                               Value
----                               -
TSPEC ADDTS Request                 0
TSPEC accepted                       0
TSPEC denied due to CAC              0
TSPEC enforcement timer events       0
Calls established within enforcement 0
TSPEC deleted after enforcement      0
period
```

Related Commands

Command	Description
ap wired-ap-profile	This command configures a wired AP profile.
show ap config	This command shows a large list of configuration settings for an ap-group or an individual AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms ap

```
show wms ap {<bssid>|list <essid> |stats [mon-mac <mon-mac> bssid <bssid>]|tree}
```

Description

This command displays information for APs currently monitored by the Wireless Management System (WMS). The WMS feature periodically sends statistics that it has collected for APs and Probes to the WMS process. When WMS receives an event message from an AM, it will save the event information along with the BSSID of the AP that generated the event in the WMS database. When WMS receives statistics from the AM, it updates its state, and the database.

Parameter	Description
<bssid>	Enter the AP's BSSID number in hexadecimal format (XX:XX:XX:XX:XX:XX).
list	Shows the list of all APs monitored by WMS.
<essid>	Shows the details of that particular ESSID.
stats	Shows the AP Statistics table for all APs.
mon-mac <mon-mac>	Shows the AP Tree table for an AP with the specified MAC address.
bssid <bssid>	Shows the AP Tree table for an AP with the specified BSSID.
tree	Show the APs seen by each monitoring probe in the WMS.

Examples

The following example displays a list of AP MAC addresses and the BSSIDs seen by each AP along with reclassification of the monitored AP triggered by the user:

```
(host) [mynode] #show wms ap 00:0d:67:20:db:4b
AP Info
-----
BSSID      SSID  Channel  Type          RAP_Type          Status
Ageout    HT-Type  HT-Sec-Chan
-----  -----  -----  -----  -----  -----
70:3a:0e:6e:2a:71      64      generic-ap  suspected-rogue (40%)  up
-1      VHT-80mhz  0

Match Info
-----
Match-Type      Match-Source  Match-Time
```

```

-----
Manual          admin          Thu Oct 22 12:05:56 2020

Probe Info
-----
MAC             IP             Name           Type
Status  AP Type
---          --          ----          ----
-----          -----
ac:a3:1e:57:82:50  10.65.47.250  ac:a3:1e:cd:78:24  soft-ap
up          325
f4:2e:7f:0b:a8:90  2001:330::f62e:7fff:fec8:ba88  zren515          soft-ap
up          515

```

The output of this command includes the following parameters:

Column	Description
AP Info	
BSSID	Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
SSID	The Service Set Identifier (SSID) that identifies a wireless network.
Channel	Channel used by the AP radio.
Type	A WMS AP type can be one of the following: <ul style="list-style-type: none"> ▪ soft-ap: An Aruba Access Point (AP). ▪ air-monitor: An Aruba Air Monitor (AM).
RAP_Type	Indicates one of the following Rogue AP types: <ul style="list-style-type: none"> ▪ Valid (not a rogue AP) ▪ Interfering ▪ Rogue ▪ Suspected Rogue ▪ Disabled Rogue ▪ Unclassified ▪ Known Interfering
Status	If up, the AP is active. If down (or no information is shown) the AP is inactive.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a -1, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
HT-type	The type of high-throughput traffic sent by the AP:

Column	Description
	<ul style="list-style-type: none"> ▪ HT-20mhz: The AP radio uses a single 20 MHz channel ▪ HT-40mhz: The AP radio uses a 40 MHz channel pair comprised of two adjacent 20 MHz channels.
HT-Sec-Chan	Secondary channel used for 40 MHz high-throughput transmissions.
Match Info	
<p>NOTE: Depending on the match type or the classification, the Match Info table may be displayed containing all or some of the following fields:</p>	
Match-Type	Indicates the type of matching detected by the AP.
Match-Source	Indicates the source of the manual reclassification. This field is displayed only when the AP has the match type Manual .
Match-Time	Indicates the time of matching for any match type.
Rule-Name	Indicates the AP classification rule name defined by the user.
Helper-BSSID	
Match-Method	Indicates the condition used to match the discovered AP with the match type.
Match-MAC	Indicates the MAC address of a wired device that helped identify the AP as rogue or suspected-rogue. If the AP has not been identified as a rogue, this column displays the MAC address 00:00:00:00:00:00 .
Match-AP	Indicates the valid AP name that matches successfully with the AP classification.
Probe Info	
MAC	MAC address of a probe that can see the specified AP.
IP	IP address of a probe that can see the specified AP.
Name	Name of the probe.
Type	Displays the probe type: A WMS probe can be one of the following: <ul style="list-style-type: none"> ▪ soft-ap: An Aruba Access Point (AP). ▪ air-monitor: An Aruba Air Monitor (AM).
Status	If up, the AP is active. If down (or no information is shown) the AP is inactive.
AP Type	AP model type.

The following example displays received and transmitted data statistics for each BSSID seen by a monitoring AP. (For versions prior to ArubaOS 8.9.0.0)

```
(host) [mynode] # show wms ap list
AP List
-----
BSSID          ESSID          Class
PHY Type      AP-name      Encryp      IBSS  Last Mon Eth MAC  Match Type
-----
Match Source  Match Time
-----
-----
80:8d:b7:82:5e:90 yfjiang_default interfering
80211A         unknown      no          ac:a3:1e:cd:78:24 None
                Wed Oct 21 11:31:16 2020

70:3a:0e:4e:e8:f2 fd1_mac_auth   suspected-rogue (20%)
80211A         open         no          f4:2e:7f:c8:ba:88 Eth-Prop-
Wired-Mac      Thu Oct 22 12:08:07 2020

38:17:c3:85:71:73          interfering
80211A         wpa3-owe-aes no          ac:a3:1e:cd:78:24 None
                Thu Oct 22 13:34:19 2020

38:17:c3:ff:f9:70 24ed646eb71fdfaa33f99db32d02da9 interfering
80211A         wpa2-psk-aes no          f4:2e:7f:c8:ba:88 None
                Thu Oct 22 12:14:03 2020

f0:5c:19:21:ad:b1          interfering
80211A         wpa2-psk-aes no          f4:2e:7f:c8:ba:88 None
                Thu Oct 22 13:04:48 2020

ac:a3:1e:c9:41:30 000-booth-guest-205 interfering
80211A         open         no          ac:a3:1e:cd:78:24 None
                Thu Oct 22 13:34:19 2020

80:8d:b7:82:5b:1e yingli-1      interfering
80211A         wpa2-psk-aes no          ac:a3:1e:cd:78:24 None
                Wed Oct 21 11:40:15 2020
```

Starting from ArubaOS 8.9.0.0, the output of the show wms ap list command can be filtered based on the ESSIDs. The following command displays information related to an ESSID, **host**.

```
(host) [mynode] # show wms ap list host
AP List
-----
BSSID          ESSID          Class          Band          AP-
name
-----
-----
```

```

-
80:8d:b7:82:5e:90  host                interfering                5GHz

Encryp            IBSS  Last Mon Eth MAC  Match Type                Match Source
Match Time
-----
-----
unknown          no    ac:a3:1e:cd:78:24  None
Wed Oct 21 11:31:16

```

The output of this command includes the following parameters:

Column	Description
BSSID	MAC address of an AP.
ESSID	The Extended Service Set Identifier (SSID) that identifies a wireless network.
Class	The classification of the monitored AP. Following are the classification types: <ul style="list-style-type: none"> valid interfering suspected-rogue neighbor rogue manually-contained
PHY Type (For versions prior to ArubaOS 8.9.0.0)	Displays one of the following radio bands: <ul style="list-style-type: none"> 802.11a 802.11b 802.11g 802.11ag
Band (ArubaOS 8.9.0.0 or later versions)	Displays one of the following radio bands: <ul style="list-style-type: none"> 2.4GHz 5GHz 6GHz
AP-name	Name of the AP.
Encryp	Encryption type used on each listed AP.

Column	Description
IBSS	Displays if ad hoc BSS is enabled or disabled on each listed AP.
Last Mon Eth MAC	Displays the last monitored MAC address seen on the wired network for the AP.
Match-Type	Indicates the type of matching detected by the AP.
Match-Source	Indicates the source of the manual reclassification. This field displays information only when the classification is manual.
Match-Time	Indicates the time of matching for manual or any other match type.

The following example displays received and transmitted data statistics for each BSSID seen by a monitored AP.

```
(host) [mynode] # show wms ap stats
AP Stats Table
-----
Monitor-MAC      BSSID           RSSI  TxPkt   RxPkt   TxByte
RxByte    HTRates-Tx
-----
---
00:0b:86:c1:af:20 00:0b:86:9a:f2:00 12    1575675  65     173239998  9340
0
00:0b:86:c1:af:20 00:0b:86:9a:f2:08 12    1560559  0     162297938  0
0
00:0b:86:c1:be:56 00:0b:86:9b:e5:60 12    1683013  4188   184400159
257583  0
00:0b:86:c1:be:56 00:0b:86:9b:e5:68 12    1580152  105    164216336  1470
0
00:0b:86:c2:0a:98 00:0b:86:a0:a9:80 48    1608023  40596  166962148
568386  0
00:0b:86:c2:1c:08 00:0b:86:a1:c0:80 42    1587097  26236  164904668
453196  0
00:0b:86:c2:1c:38 00:0b:86:a1:c3:80 42    1573040  20511  174536514
654024  0
00:0b:86:c2:3e:a9 00:0b:86:a3:ea:90 48    1588204  34179  165017293
897431  0
00:0b:86:c4:0f:3c 00:0b:86:c0:f3:d0 48    1571202  14258  174338376
351148  0
00:0b:86:c4:4d:06 00:0b:86:c4:d0:70 48    1598423  56198  182267018
3805826  0
00:1a:1e:c0:88:82 00:1a:1e:88:88:30 18    1717310  247532 394461405
14998234  8
00:1a:1e:c0:88:82 00:1a:1e:88:88:20 18    1092023  114722 242006054
2442917  10
```

```

00:1a:1e:c0:88:88 00:1a:1e:88:88:90 36 1783226 485620 460219125
27781583 16
HTRates-Rx
-----
0
0
0
0
0
0
0
0
0
0
0
8
10
16

```

The output of this command includes the following parameters:

Column	Description
Monitor-MAC	MAC address of an AP.
BSSID	Basic Service Set Identifier (BSSID) of a station.
RSSI	Received Signal Strength Indicator (RSSI) for the station, as seen by the AP.
txPkt	Number of transmitted packets.
RxPkt	Number of received packets.
TxByte	Number of transmitted bytes.
RxByte	Number of received bytes.
HTRates-Tx	Number of bytes transmitted at high-throughput rates.
HTRates-Rx	Number of bytes received at high-throughput rates.

Related Command

Command	Description
wms ap	This command allows you to classify an AP into one of the several categories.

Command History

Release	Modification
ArubaOS 8.9.0.0	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> ■ The output of the <code>show wms ap list</code> command can be filtered based on the ESSIDs. ■ Introduced <code>Band</code> parameter in the output of the <code>show wms ap list</code> and <code>show wms ap tree</code> commands. ■ Introduced the 2.4GHz, 5GHz, and 6GHz values under <code>Band</code> parameter.
ArubaOS 8.8.0.0	<p>The following parameters were added to the output of the <code>show wms ap <bssid></code> and <code>show wms ap list</code> commands:</p> <ul style="list-style-type: none"> ■ Match-Type ■ Match-Source ■ Match-Time
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms channel

```
show wms channel stats <num>
```

Description

This command displays per-channel statistics for monitored APs.

Parameter	Description
<num>	Channel number.

Example

The following example shows per-channel statistics for monitored APs:

```
(host) [mynode] #show wms channel stats
Channel Stats Table
-----
Monitor-MAC      Channel  NumAP  NumSta  TotalPkt  TotalByte  Noise
-----
00:0b:86:c1:af:20  1        1      0       5228276   613640650  97
00:0b:86:c1:af:20  6        1      0       1355     168764    0
00:0b:86:c1:af:20  11       8      0       5880     1040338   0
00:0b:86:c1:af:20  36       0      0        2        28        0
00:0b:86:c1:af:20  40       0      0        2       112       0
00:0b:86:c1:af:20  44       0      0        50       903       0
00:0b:86:c1:af:20  48       0      0        23       544       0
00:0b:86:c1:af:20  149      1      0       27094    557579    0
00:0b:86:c1:af:20  153      3      0      4648662  544817261 99
00:0b:86:c1:af:20  165      1      0       1655     200349    0
00:0b:86:c1:be:56  1        43     4      14446324 1959058619 0
00:0b:86:c1:be:56  6        8      1      14168505 1955474600 96
00:0b:86:c1:be:56  11       72     1      180553   23987119  0
00:0b:86:c1:be:56  36       53     0      14716    1022825   0
00:0b:86:c1:be:56  40       8      0      3033     501568    0
00:0b:86:c1:be:56  44       3      0      1453     217596    0
00:0b:86:c1:be:56  48       4      0      5330     1067660   0
00:0b:86:c1:be:56  149      0      0      609279   72205247  105
00:0b:86:c1:be:56  153      1      0      7615369  779579648 0
00:0b:86:c1:be:56  165      1      0      4238     486121    0
00:0b:86:c2:0a:98  40       4      0      4247     434512    0
00:0b:86:c2:0a:98  48       5      0      4052     420436    0
00:0b:86:c2:0a:98  149      4      0      6548323  732910481 104
00:0b:86:c2:1c:08  40       3      0      4613     478188    0
00:0b:86:c2:1c:08  48       4      0      6235436  658263321 103
00:0b:86:c2:1c:08  149      5      0      18904    803078    0
```

Column	Description
Monitor-MAC	MAC address of an AP.
Channel	802.11 radio channel.
NumAP	Number of other APs seen on the specified channel.
NumSta	Number stations seen on the specified channel.
TotalPkt	Number of received packets.
TotalByte	Number of received bytes.
Noise	Current noise level.

Related Commands

Command	Description
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms client

```
show wms client {list|<mac>|probe <mac>|stats [mon-mac <mon-mac> mac <mac>]|tree|valid-exempt}
```

Description

This command displays the list of client information for the clients that can be seen by monitoring APs.

Parameter	Description
list	Show statistics for all monitored clients.
<mac>	Show statistics for a client with the specified MAC address, including the BSSID of the AP to which that client is currently associated, and the MAC addresses of other monitoring APs that can see that client.
probe <mac>	Specify a client's MAC address to show the BSSIDs of all probes that can see that client.
stats	Show the STA stats table, which displays data for all clients seen by each monitoring AP.
mon-mac <mon-mac> mac <mac>	Enter a monitoring AP's MAC address (<mon-mac>) and the MAC address of a client (<mac>) to show data for traffic received from and sent to a specific client as seen by a specific AP.
tree	Shows a list of the clients seen by each monitoring probe.
valid-exempt	Shows a list of valid-exempt clients.

Example

The following example shows statistics for a client with the specified MAC address, including the BSSID of the AP to which that client is currently associated with. The **AP Info** table in the example below shows that the client is associated to an AP with the BSSID **00:0b:86:cd:86:a0**. The **Probe Info** table shows the MAC addresses of three other APs that can see the client. (For versions prior to ArubaOS 8.9.0.0)

```
(host) [mynode] #show wms client 00:0e:35:29:9b:28
Probe Info
-----
MAC                Type   Status  Ageout  HT-Type
---                -
00:0e:35:29:9b:28  valid  up      -1      HT-40mhz
```

```

AP Info
-----
BSSID          SSID      Channel  Type      RAP_Type  Status  Ageout
HT-Type      HT-Sec-Chan
-----
00:0b:86:cd:86:a0  MySSID  11      soft-ap  valid     up      -1
HT-40mhz    153

```

In the following example, the **AP Info** table also shows the radio band along with the channel used by the radio, the high-throughput traffic sent by the AP, and the secondary channel used for high-throughput transmissions. (ArubaOS 8.9.0.0 or later versions)

```

(host) [mynode] #show wms client 84:d4:7e:e6:17:50

AP Info
-----
BSSID          SSID          Band/Chan/HT-Type/HT-Sec-Chan  Type
RAP_Type  Status  Ageout
-----
84:d4:7e:e6:17:50  9@hbm-535-rtp  5GHz/52/-/-  soft-ap
valid      up      1
Probe Info
-----
MAC          IP      Name      Type      Status  AP Type
-----
84:d4:7e:e6:17:50  1.1.1.6  qc-225  soft-ap  up      225

```

The output of this command includes some or all of the following parameters.

Column	Description
MAC	MAC address of a WMS probe.
Type	Station type (valid , interfering , or disabled rogue client).

Column	Description
Status	If up , the client is active. If down (or no information is shown) the client is inactive.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a -1 , the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
BSSID	BSSID of the AP to which the client is associated.
SSID	Extended service set identifier (ESSID) of the BSSID.
Channel (For versions prior to ArubaOS 8.9.0.0)	Channel used by the AP radio.
Type	<p>A WMS AP type can be one of the following:</p> <ul style="list-style-type: none"> ▪ soft-ap: Aruba Access Point (AP). ▪ air-monitor: Aruba Air Monitor (AM).

Column	Description
RAP_Type	<p>Indicates one of the following Rogue AP types:</p> <ul style="list-style-type: none"> ▪ Valid (not a rogue AP) ▪ Interfering ▪ Rogue ▪ Disabled Rogue ▪ Suspected Rogue ▪ Unclassified ▪ Known Interfering
Status	<p>If up, the AP is active. If down (or no information is shown) the AP is inactive.</p>
Ageout	<p>An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a -1, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.</p>
HT-Type (For versions prior to ArubaOS 8.9.0.0)	<p>Type of high-throughput traffic sent by the AP.</p>
HT-Sec-Chan (For versions prior to ArubaOS 8.9.0.0)	<p>Secondary channel used for high-throughput transmissions.</p>

Column	Description
Band/Chan/HT-Type/HT-Sec-Chan (ArubaOS 8.9.0.0 or later versions)	Displays information in the order of the radio band/radio channel/high-throughput traffic type/secondary channel used for high-throughput traffic.
IP	IP address of a WMS probe.
AP type	Model type of the probe.

The following example lists the statistics for all monitored clients. (ArubaOS 8.9.0.0 or later versions)

```
(host) [mynode] (config) #show wms client list

Station List
-----
MAC          BSSID          ESSID   Class          Band  Last Mon
Eth MAC
---          -
-----
fc:b3:bc:45:36:de  1c:28:af:68:28:c2  ssid-1  interfering    6GHz
cc:88:c7:cc:16:46
Total:1
```

The output of this command includes the following parameters.

Column	Description
MAC	MAC address of the client.
BSSID	BSSID of the AP to which the client is associated.
ESSID	Extended service set identifier (ESSID) of the BSSID.
Class	The classification of the monitored AP. Following are the classification types: <ul style="list-style-type: none"> ■ valid ■ interfering ■ suspected-rogue ■ neighbor ■ rogue ■ manually-contained

Column	Description
Band	The AP radio band. Following are the possible values: <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz
Last Mon Eth MAC	The last monitored MAC address seen on the wired network for the AP.

Related Commands

Command	Description
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.9.0.0	The command output was modified to include the following changes: (ArubaOS 8.9.0.0 or later versions) <ul style="list-style-type: none"> ■ Introduced <code>Band</code> parameter in the output of <code>show wms client list</code> command. ■ Introduced <code>Band/Chan/HT-Type/HT-Sec-Chan</code> parameter in the output of <code>show wms client <mac></code> command. ■ Introduced the 2.4GHz, 5GHz, and 6GHz values under <code>Band</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms counters

```
show wms counters [debug|events|rap-ack]
```

Description

This command displays WMS events and debug counters. If you omit the optional `debug` and `events` parameters, the `show wms counters` command displays the frequently used (general) counters in a single table. This command displays counters for database entries, messages, and data structures. The counters displayed vary for each managed device; if the managed device does not have an entry for a particular counter type, it does not appear in the output of this command.

Parameter	Description
<code>debug</code>	Displays debug counters only.
<code>events</code>	Displays events counters only.
<code>rap-ack</code>	Displays number of pending PROBE_RAP_ACK for each probe.

Example

The following example shows output for the `show wms counters` command:

```
(host) [mynode] #show wms counters
Counters
-----
Name                               Value
----                               -
DB Reads                           288268
DB Writes                           350870
Probe Table DB Reads                2477
Probe Table DB Writes                952
AP Table DB Reads                   143992
AP Table DB Writes                   138867
STA Table DB Reads                   40404
STA Table DB Writes                  99687
Probe STA Table DB Reads             101352
Probe STA Table DB Writes            117566
Probe Register                       2476
Probe State Update                   37077
Set RAP Type                         42552
Set RAP Type Conf Level              152
Valid Exempt Station Macs           10
...
```

Related Commands

Command	Description
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms forwarding-stats

```
show wms forwarding-stats
```

Description

This command displays message forwarding statistics between the WLAN Management System (WMS) and Aruba Air Monitor.

Example

The following command displays forwarding statistics between the WMS and Air Monitor:

```
(host) [mynode] #show wms forwarding-stats
WMS Forwarding Stats
-----
Item                               Value
----                               -
Messages Forwarded                 10
Messages Dropped                   1
Messages Diverted to Local Processing 0
```

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms general

show wms general [debug]

Description

This command displays general configuration information for the Aruba WLAN Management System (WMS).

Parameter	Description
debug	Displays general debugging information for WMS.

Example

The following command displays general configuration information for WMS:

```
(host) [mynode] #show wms general
General Attributes
-----
Key                               Value
---                               -
poll-interval                     60000
poll-retries                       2
ap-ageout-interval                 30
adhoc-ap-ageout-interval           5
sta-ageout-interval                 30
learn-ap                           disable
persistent-neighbor                enable
persistent-valid-sta               disable
propagate-wired-macs               enable
learn-system-wired-macs            disable
stat-update                         disable
collect-stats                      disable
classification-server-ip            0.0.0.0
rtls-port                           8000
wms-on-master/conductor              enable
event-correlation                   logs-and-traps
event-correlation-quiet-time        900
use-db                              enable
calc-poll-interval                 60000
Switch IP                           192.192.192.1
Services IP                         192.192.192.10
Controller Svcs Role                 Svc Master/Conductor
Is WMS Master/Conductor              enable
Minutes Tick                         10516
```

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>master</code> have been replaced with <code>conductor</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

Command History

Release	Release
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms probe

show wms probe

Description

This command displays detailed information on WMS probes.

Example

The following example shows the Probe List table for WMS probes. (For versions prior to ArubaOS 8.9.0.0)

```
(host) [mynode] #show wms probe
Probe List
-----
Monitor Eth MAC      BSSID              PHY Type           IP                LMS
IP          Scan  Status  Updates  Reqs/Fails  Stats  Type
-----
--
40:e3:d6:cf:61:96    40:e3:d6:76:19:60  80211GHT-20mhz    191.191.191.252
192.192.189.1 No    Up      6850     1/0         0      soft-ap
40:e3:d6:cf:61:96    40:e3:d6:76:19:70  80211AVHT-80mhz   191.191.191.252
192.192.189.1 No    Up      6860     0/0         0      soft-ap
40:e3:d6:c0:dc:ae    40:e3:d6:8d:ca:e0  80211GHT-20mhz    191.191.191.253
192.192.189.1 No    Up      6924     1/0         0      soft-ap
40:e3:d6:c0:dc:ae    40:e3:d6:8d:ca:f0  80211AVHT-80mhz   191.191.191.253
192.192.189.1 No    Up      6909     0/0         0      soft-ap
Total:4
```

The following example shows the Probe List table for WMS probes. (ArubaOS 8.9.0.0 or later versions)

```
(host) [mynode] #show wms probe
Probe List
-----
Monitor Eth MAC      BSSID              Band/HT-Type       IP                LMS IP
IP          Scan  Status  Updates  Reqs/Fails  Stats  Type
-----
--
20:4c:03:0e:bc:d6    f0:5c:19:1d:d5:d0  2.4GHz/HT-20mhz    1.1.1.10
10.65.47.6 No    Down    0         0/0         0      soft-ap
1c:28:af:ce:81:03    1c:28:af:68:10:40  5GHz/VHT-80mhz     10.65.47.27
10.65.47.6 No    Down    0         0/0         0      air-monitor
94:b4:0f:c1:54:18    94:b4:0f:95:41:90  5GHz/VHT-80mhz     1.1.1.17
10.65.47.6 No    Down    0         0/0         0      soft-ap
9c:8c:d8:cf:f9:1a    9c:8c:d8:7f:91:c0  2.4GHz/HE-20mhz    10.65.36.141
10.65.47.6 No    Down    0         0/0         0      soft-ap
```

```

9c:8c:d8:cf:f6:95 9c:8c:d8:7f:69:70 2.4GHz/HE-20mhz 10.65.36.137
10.65.47.6 No Down 0 0/0 0 soft-ap
20:4c:03:0e:bc:d6 f0:5c:19:1d:d5:c0 5GHz/HT-20mhz 1.1.1.14
10.65.47.6 No Down 0 0/0 0 soft-ap
9c:8c:d8:cf:f9:6e 9c:8c:d8:7f:96:f0 5GHz/HE-80mhz 10.65.47.29
10.65.47.6 No Down 18287 3/1 0 soft-ap
94:b4:0f:c1:54:18 94:b4:0f:95:41:80 2.4GHz/HT-20mhz 1.1.1.6
10.65.47.6 No Down 0 0/0 0 soft-ap
ac:a3:1e:c5:26:8a ac:a3:1e:d2:68:b0 5GHz/VHT-80mhz 1.1.1.18
10.65.47.6 No Down 0 0/0 0 soft-ap
Total:9

```

Column	Description
Monitor Eth MAC	Ethernet MAC address of a probe.
BSSID	Probe Radio BSSID.
PHY Type (For versions prior to ArubaOS 8.9.0.0)	Radio PHY type: <ul style="list-style-type: none"> ■ 802.11A ■ 802.11AHT-40Mbps ■ 802.11AHT-20Mbps ■ 802.11G ■ 802,11GHT-20Mbps
Band/HT-Type (ArubaOS 8.9.0.0 or later versions)	The radio band and the high-throughput traffic type sent by the AP. Displays one of the following radio bands: <ul style="list-style-type: none"> ■ 2.4GHz ■ 5GHz ■ 6GHz
IP	IP address of the AP.
LMS IP	IP address of the AP's managed device.
Scan	Shows if the Air Monitor is performing scanning.
Status	If the scan column displays a status of Up, the AP or AM is active
Updates	Number of updates the AP or AM sent to the WMS database since the managed device was last reset.

Column	Description
Reqs/Fails	Number of database update requests that have not yet been added into the database, and the number of failed database requests.
Stats	Total number of statistics updates sent to the database.
Type	A WMS AP type can be one of the following: <ul style="list-style-type: none"> ▪ soft-ap: An Aruba Access Point (AP). ▪ air-monitor: An Aruba Air Monitor (AM).

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Release
ArubaOS 8.9.0.0	The command output was modified to include the following changes: (ArubaOS 8.9.0.0 or later versions) <ul style="list-style-type: none"> ▪ Introduced <code>Band/HT-Type</code> parameter. ▪ Introduced the 2.4GHz, 5GHz, and 6GHz values under <code>Band</code> parameter.
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms rogue-ap

```
show wms rogue-ap <bssid> [list]
```

Description

This command displays statistics for APs classified as rogues APs. The optional output modifiers `begin`, `exclude`, and `include` help you display those lines that begin, include, and exclude respectively, the line expression given in the CLI command. The `redirect-output` modifier helps you redirect the command output.

Parameter	Description
<bssid>	BSSID of a rogue AP.
list	Shows rogue AP list.

Examples

The following example shows statistics for a suspected rogue AP based on the BSSID.

```
(host) [mynode] #show wms rogue-ap 00:0b:86:d4:ca:12
Suspect Rogue AP Info
-----
Key                Value
---                -
BSSID              00:0b:86:d4:ca:12
SSID               aruba-ap
Band/Chan/HT-Type/HT-Sec-Chan 5GHz/36/VHT-80mhz/-
Type               generic-ap
RAP Type           suspected-rogue
Status             up
Match Type         AP-Rule
Match MAC          00:0b:86:61:8a:d0
Match IPv4         0.0.0.0
Match IPv6         0.0.0.0
Match AM           ssahoo-155
Match Method       Exact-Match
Helper AP BSSID    a8:bd:27:22:8b:70
Match Time         Sun Sep 19 19:11:40 2010
```

The output of this command includes the following information:

Column	Description
BSSID	BSSID of the suspected rogue AP.

Column	Description
SSID	The rogue AP's Extended service set identifier.
Channel (For versions prior to ArubaOS 8.9.0.0)	Channel used by a radio on the rogue AP.
Band/Chan/HT-Type/HT-Sec-Chan (ArubaOS 8.9.0.0 or later versions)	Displays information in the order of the radio band/radio channel/high-throughput traffic type/secondary channel used for high-throughput traffic.
Type	Indicates if the AP is an Aruba AP, a Cisco AP, or an AP from any other manufacturer (generic AP).
RAP Type	Type of rogue AP, <ul style="list-style-type: none"> ▪ Suspect-unsecure: AP has not been confirmed as a rogue AP. ▪ unsecure: AP has been confirmed as a rogue AP.
Status	Shows if the AP is active (up) or inactive (down).
Match Type	Describes how the AP was classified as a rogue. <ul style="list-style-type: none"> ▪ Eth-Wired-MAC: An Aruba AP or AM detected that a single MAC address was in both the Ethernet Wired-Mac table and a non-valid AP wired-Mac table. ▪ AP-Wired-MAC: An interfering AP is marked as rogue when the Aruba AP finds a MAC address in one of its valid AP wired-mac table and in an interfering AP wired-mac table. You can enable or disable the AP-Wired-MAC matching method using the CLI command ids unauthorized-device-profile overlay-classification. ▪ Config-Wired-MAC: This type of classification occurs when an Aruba AP or AM detects a match between a wired MAC table and a pre-defined MAC address that has manually defined via the command ids unauthorized-device-profile . ▪ External-Wired-MAC: This type of classification occurs when an Aruba AP or AM detects a match between a wired MAC table entry and a pre-defined MAC address manually defined in the ids rap-wml-server-profile table.

Column	Description
	<ul style="list-style-type: none"> ▪ Base-BSSID-Override: If an Aruba AP is detected as rogue, then all virtual APs on the particular rogue are marked as rogue using Base-BSSID-Override match type. ▪ Manual: An AP is manually defined as a rogue by via the command <code>wms ap <bssid> mode rogue</code>. ▪ EMS: An AP is manually defined as a rogue by via the Element Management System.
Match MAC	MAC address of a wired device that helped identify the AP as a rogue. If the AP has not been identified as a rogue, this column will display the MAC address 00:00:00:00:00:00.
Match IPv4	IPv4 address of a wired device that helped identify the AP as a rogue.
Match IPv6	IPv6 address of a wired device that helped identify the AP as a rogue.
Match AM	Aruba Air Monitor that reported seeing the rogue AP.
Match Method	This variable indicates the type of match.
Match Time	Time the AP was identified as a rogue AP.

The following example shows statistics for a suspected rogue AP list. (ArubaOS 8.9.0.0 or later versions)

```
(host) [mynode] (config) #show wms rogue-ap list

AP List
-----
BSSID          ESSID    Class      Band  AP-name  Encryp  IBSS  Last
Mon Eth MAC   Match  Type  Match Source  Match Time
-----
-----
1c:28:af:68:28:c2  ssid-1  interfering 6GHz  hhm-635  unknown no
ac:a3:1e:cd:78:24 None                               Wed Oct 21 11:31:16
Total:1
```

The output of this command includes the following parameters:

Column	Description
BSSID	MAC address of an AP.
ESSID	The Extended Service Set Identifier (SSID) that identifies a wireless network.
Class	The classification of the monitored AP. Following are the classification types: <ul style="list-style-type: none"> ▪ valid ▪ interfering ▪ suspected-rogue ▪ neighbor ▪ rogue ▪ manually-contained
Band	The AP radio band. Following are the possible values: <ul style="list-style-type: none"> ▪ 2.4GHz ▪ 5GHz ▪ 6GHz
AP-name	Name of the AP.
Encryp	Encryption type used on each listed AP.
IBSS	Displays if ad hoc BSS is enabled or disabled on each listed AP.
Last Mon Eth MAC	Displays the last monitored MAC address seen on the wired network for the AP.
Match-Type	Indicates the type of matching detected by the AP.
Match-Source	Indicates the source of the manual reclassification. This field displays information only when the classification is manual.
Match-Time	Indicates the time of matching for manual or any other match type.

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.9.0.0	<p>The command outputs were modified to include the following changes: (ArubaOS 8.9.0.0 or later versions)</p> <ul style="list-style-type: none"> ■ Introduced <code>Band</code> parameter under <code>show wms rogue-ap list</code> command. ■ Introduced the 2.4GHz, 5GHz, and 6GHz values under <code>Band</code> parameter. ■ Introduced <code>Band/Chan/HT-Type/HT-Sec-Chan</code> parameter under <code>show wms rogue-ap <bssid></code> command.
ArubaOS 8.7.0.0	<p>The output of the <code>show wms rogue-ap <bssid></code> command was modified to display the following fields:</p> <ul style="list-style-type: none"> ■ Match IPv4 ■ Match IPv6
ArubaOS 8.2.0.0	The <code>list</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms rogue-ap list

```
show wms rogue-ap list
```

Description

This command displays the information on the rogue APs in the network. When an AM classifies an interfering AP as a Rogue AP it sends that classification to the WMS process.

Use this command to list all known Rogue APs that may be potential security threats.

Examples

The `show wms rogue-ap list` command displays a list of rogue APs detected in the network.

```
(host)[mynode] #show wms rogue-ap list
AP List
-----
BSSID          ESSID          Class  PHY Type AP-name Encryp      IBSS  Last
Mon Eth MAC
-----
-----
ac:a3:1e:53:72:94 arturo04       rogue  80211A          wpa2-psk-aes  no
ac:a3:1e:cd:35:5a
84:d4:7e:64:1c:72 hpeguest      rogue  80211A          open           no
ac:a3:1e:cd:35:5a
00:62:ec:26:2e:2f smtcwireless  rogue  80211A          wpa-8021x-tkip no
c8:b5:ad:c3:ac:fc
Total: 3
```

The output of this command includes the following information:

Column	Description
BSSID	Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
ESSID	The Extended Service Set Identifier (SSID) that identifies a wireless network.
Class	AP classification: will always be set to 'rogue'. A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.
PHY Type	Shows one of the following 802.11 types: <ul style="list-style-type: none">802.11a802.11b802..11g

Column	Description
	<ul style="list-style-type: none"> 802.11 ag
AP-name	Name of the rogue AP.
Encryp	Encryption type used on each listed rogue AP.
IBSS	Shows if ad hoc BSS is enabled or disabled on each listed rogue AP.
Last Mon Eth MAC	Shows the last monitored MAC address seen on the wired network for this rogue AP.

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the controller or managed device.

show wms routers

```
show wms routers [<mac>]
```

Description

This command displays learned router MAC information for WMS APs. This command displays the MAC addresses of devices that have been determined to be routers by the listed APs. This output of this command will be blank if there is not any broadcast or multicast activity in an AP's subnet.

Parameter	Description
<mac>	MAC address of a probe that can see the router.

Example

In the example below, a single WMS AP has learned MAC information for four different routers.

```
(host) [mynode] #show wms routers
Router Mac 00:08:00:00:11:12 is Seen by APs
-----
AP-Name
-----
AP32
Router Mac 00:08:00:00:11:29 is Seen by APs
-----
AP-Name
-----
AP32
Router Mac 00:08:00:00:11:57 is Seen by APs
-----
AP-Name
-----
AP32
Router Mac 00:08:00:00:11:6e is Seen by APs
-----
AP-Name
-----
AP32
```

Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms rules

```
show wms rules
  config
  state
  summary
```

Description

This command displays the internal state and matching information of rules created using the [ids ap-classification-rule](#) command. Issue this command to view existing AP classification rules. AP classification rule configuration can only be performed on a Mobility Conductor. If AMP is enabled via the mobility-manager command, then processing of the AP classification rules is disabled on Mobility Conductor. A rule is identified by its ASCII character string name (32 characters maximum).

The AP classification rules have one of the following specifications:

- SSID of the AP
- SNR of the AP
- Discovered-AP-Count or the number of APs that can see the AP

Parameter	Description
config	Displays the following information for each AP classification rule: <ul style="list-style-type: none">▪ name▪ ids▪ match-ssid▪ min-snr▪ max-snr▪ min-prcnt▪ max-prcnt▪ ssids▪ enabled▪ classify▪ conf-incr▪ flags▪ match-cnt
state	Displays the following information for each AP classification rule: <ul style="list-style-type: none">▪ SSID Match Table▪ SSID Exclude Table▪ SNR Table▪ Probe Count Table
summary	Displays a summary of AP classification rules.

Example

The output in the example below shows that although two rules have been defined, neither have been enabled using the `ids ap-rule-matching rule-name <name>` command.

```
(host) [mynode] #show wms rules summary
AP Classification Rules Summary
-----
Parameter                Value
-----
Num Rules                 2
Num Active-Rules         0
Num SSID-to-match        0
Num SSID-to-exclude      0
Num SNR-bounds           0
Num Probe-Count-bounds  0
```

Related Commands

Command	Description
wms client	This command configures the IDS AP classification rule profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wms system

```
show wms system
```

Description

This command displays the WMS system configuration and system state.

Example

The following example shows the WMS System Configuration and System State tables:

```
(host) [mynode] #show wms system

System Configuration
-----
Key                               Value
---                               -
max-ap-threshold                  0
max-sta-threshold                 0
max-rbtree-entries               0
max-system-wm                    1000
system-wm-update-interval        8
periodic-ap-snapshot-interval    180
periodic-rap-snapshot-interval   30
periodic-sta-snapshot-interval   180
override-svc-termination         disable
System State
-----
Key                               Value
---                               -
Max AP Threshold                  250000
Max STA Threshold                 750000
Total AP Count                   371
Total STA Count                  14
Max RB-tree Threshold            2000000
Current RB-Tree Count            530
Poll Count (Max)                 1 (4)
WMS Offload State
-----
Metric                            Threshold  Current
-----
AP Count                          200000   371
STA Count                          600000   14
RB-Tree Count                     1600000  530
Probe Count                        20000    4
WMS Offload: Disabled
Learned OUIs for Deployed APs
-----
OUI
---
40:e3:d6:00:00:00
```


Related Commands

Command	Description
wms ap	This command allows you to classify an AP into one of several categories.
wms client	This command allows you to classify a wireless client into one of several categories.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show wms wired-mac

```
show wms wired-mac {gw-mac [<mac>]|monitored-ap-wm [<mac>]|prop-eth-mac  
[<mac>]|reg-ap-oui [<mac>]|summary|system-gw-mac [<mac>]|system-wired-mac  
[<mac>]|wireless-device [<mac>}}
```

Description

This command displays a summary table of WLAN Management System (WMS) wired MAC information. This command can display a list of APs aware of a specific gateway MAC address, or list the wired MAC addresses known to a single AP.

Column	Description
gw-mac	Shows gateway wired MAC information collected from the APs.
<mac>	Displays information for a single MAC address.
monitored-ap-wm	Shows monitored AP wired MAC information collected from the APs.
<mac>	Displays information for a single MAC address.
prop-eth-mac	Shows wired mac information collected from the APs.
<mac>	Displays information for a single MAC address.
reg-ap-oui	Shows registered AP OUI information collected from the APs, including each registered OUI, and the time that OUI was last seen.
<mac>	Displays information for a single MAC address.
summary	Display a wired MAC summary that includes the number of each of the following MAC types: <ul style="list-style-type: none">Registered AP OUIsPropagated Ethernet MACs.Potential Wireless Device MACsMonitored AP Wired MACsSystem Wired MACsSystem Gateway MACs
system-gw-mac	Shows system gateway MAC information learned at the managed device, including the age of each MAC address.
<mac>	Displays information for a single MAC address.

Column	Description
system-wired-mac	Shows system wired MAC information learned at the managed device.
<mac>	Displays information for a single MAC address.
wireless-device	Show routers or potential wireless devices information, including the MAC address of the device, and the MAC address of the AP or managed device that saw the device.
<mac>	Displays information for a single MAC address.

Example

The following example shows the wired MAC summary:

```
(host) [mynode] #show wms wired-mac summary
Wired MAC Summary
-----
Type                               Count
----                               -
Gateway MACs                       1
Registered AP OUIs                 16
Propagated Ethernet MACs           0
Potential Wireless Device MACs     0
Monitored AP Wired MACs             0
System Wired MACs                   0
System Gateway MACs                 0
```

Related Commands

Command	Description
clear wms wired-mac	Clear <i>learned</i> and <i>collected</i> Wired MAC information. Optionally, enter the MAC address, in nn:nn:nn:nn:nn:nn format, of the AP that has seen the Wired Mac.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show wnm-dot11v bss-tm-response

```
show wnm-dot11v bss-tm-response station-mac <mac>
```

Description

This command displays the BSS transition management response for a given client.

Column	Description
<mac>	MAC address of the client.

Example

The following example shows the BSS transition management response for a client:

```
(host) [mynode] #show wnm-dot11v bss-tm-response station-mac
58:94:6b:31:d0:f0
VLAN Assignment
-----
VLAN  #CLIENTS
----  -
1      0
192    1
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Conductor.

show ip interface brief

```
show ip interface brief
```

Description

This command displays the IP-related information on all interfaces in summary format.

Example

```
(host) #show ip interface brief
Interface                IP Address / IP Netmask      Admin  Protocol
VRRP-IP
vlan 1                   172.16.0.254 / 255.255.255.0  up     up
vlan 2                   10.4.62.9 / 255.255.255.0     up     up
loopback                 unassigned / unassigned      up     up
mgmt                    unassigned / unassigned      down   down
```

The following table details the columns and content in the show command.

Column	Description
Interface	List the interface and interface identification, where applicable.
IP Address /IP Netmask	List the IP address and netmask for the interface, if configured.
Admin	States the administrative status of the interface. Enabled—up Disabled—down
Protocol	Status of the IP on the interface. Enabled—up Disabled—down
VRRP-IP	VRRP IP address associated to the interface.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

show zigbee service-profile

```
show zigbee service-profile <profile-name>
```

Description

This command shows the ZigBee service profile.

Example

The following example shows the list of ZigBee service profiles:

```
(host) [mynode] #show zigbee service-profile

ZigBee Service Profile List
-----
Name                               References  Profile Status
----                               -
sample_zb_service_profile         0

Total:1
```

The output of this command includes the following information:

Parameter	Description
Name	Name of the ZigBee service profile.
References	Number of references to the ZigBee service profile.
Profile Status	Status of the ZigBee service profile.

The following example shows a ZigBee service profile:

```
(host) [mynode] #show zigbee service-profile sample_zb_service_profile

ZigBee Service Profile "sample_zb_service_profile"
-----
Parameter          Value
-----
Radio Instance     all
Zigbee Security    enable
Zigbee Permit Joining on
PANID              auto
```

Related Commands

Command	Description
zigbee service-profile	Configures a ZigBee service profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

show zigbee socket-device-profile

zigbee socket-device-profile <profile-name>

Description

This command shows the ZigBee socket device profile.

Example

The following example shows the list of ZigBee socket device profiles:

```
(host) [mynode] #show zigbee socket-device-profile

ZigBee Socket Device Profile List
-----
Name                               References  Profile Status
----                               -
sample_zb_socket_device_profile    0

Total:1
```

The output of this command includes the following information:

Parameter	Description
Name	Name of the ZigBee socket device profile.
References	Number of references to the ZigBee socket device profile.
Profile Status	Status of the ZigBee socket device profile.

The following example shows a ZigBee socket device profile:

```
(host) [mynode] #show zigbee device-profile sample_zb_socket_device_profile

ZigBee Socket Device Profile "sample_zb_socket_device_profile"
-----
Parameter      Value
-----
Socket Inbound  sample_zb_socket_inbound_profile
Socket Outbound sample_zb_socket_outbound_profile
```

Related Commands

Command	Description
zigbee socket-device-profile	Configures a ZigBee socket device profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

show zigbee socket-inbound-profile

zigbee socket-inbound-profile <profile-name>

Description

This command shows the ZigBee socket inbound profile.

Example

The following example shows the list of ZigBee socket inbound profiles:

```
(host) [mynode] #show zigbee socket-inbound-profile

ZigBee Socket Inbound Profile List
-----
Name                               References  Profile Status
----                               -
sample_zb_socket_inbound_profile    0

Total:1
```

The output of this command includes the following information:

Parameter	Description
Name	Name of the ZigBee socket inbound profile.
References	Number of references to the ZigBee socket inbound profile.
Profile Status	Status of the ZigBee socket inbound profile.

The following example shows a ZigBee socket inbound profile:

```
(host) [mynode] #show zigbee socket-inbound-profile sample_zb_socket_
inbound_profile

ZigBee Socket Inbound Profile "sample_zb_socket_inbound_profile"
-----
Parameter      Value
-----
Cluster ID     1234
Profile ID     0034
Endpoint       12
Source Endpoint 56
```

Related Commands

Command	Description
zigbee socket-inbound-profile	Configures the ZigBee socket inbound profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

show zigbee socket-outbound-profile

zigbee socket-outbound-profile <profile-name>

Description

This command shows the ZigBee socket outbound profile.

Example

The following example shows the list of ZigBee socket outbound profiles:

```
(host) [mynode] #show zigbee socket-outbound-profile

ZigBee Socket Outbound Profile List
-----
Name                               References  Profile Status
----                               -
sample_zb_socket_outbound_profile    0

Total:1
```

The output of this command includes the following information:

Parameter	Description
Name	Name of the ZigBee socket outbound profile.
References	Number of references to the ZigBee socket outbound profile.
Profile Status	Status of the ZigBee socket outbound profile.

The following example shows a ZigBee socket outbound profile:

```
(host) [mynode] #show zigbee socket-outbound-profile sample_zb_socket_
outbound_profile

ZigBee Socket Outbound Profile "sample_zb_socket_inbound_profile"
-----
Parameter      Value
-----
Cluster ID     1234
Profile ID     0034
Endpoint       12
Source Endpoint 56
APS Acknowledge true
```

Related Commands

Command	Description
zigbee socket-outbound-profile	Configures the ZigBee socket outbound profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

snmp-server

```
snmp-server
  community <string>
  enable
  engine-id
  host IPv4/IPv6 Address|version {1 <name> udp-port <port> [trap-group <SNMP trap
group name>]}|2c|{3 <name>}
  [inform] [interval <seconds>] [retrycount <number>] [udp-port <port>]
  [trap-group <SNMP trap group name>]}
  inform queue-length <size>
  source controller-ip
  stats
  trap {source [IPv4|IPv6 Address]|<name>}
  trap-group <SNMP trap group name>
    [snmp-server trap <trap-name>]
  user
    <word>
    [auth-prot {md5|sha} <string>]
    [priv-prot {AES|DES} <string>]
```

Description

This command configures SNMP parameters. It configures SNMP related information for APs in an SNMP profile, which is applied to an AP group or to a specific AP.

Parameter	Description
community	Sets the read-only community string.
enable	Enables sending of SNMP traps to the configured host. disabled
engine-id	Sets the SNMP server engine ID as a hexadecimal number. 24 characters maximum
host	Configures the IPv4/IPv6 Address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the controller.
version	Configures the SNMP version and security string for notification messages.
inform	Sends SNMP inform messages to the configured host. disabled

Parameter	Description
inform	Specifies the length for the SNMP inform queue. 100-350 250
stats	Allows file-based statistics collection. The Mobility Conductor/Mobility Conductor generates a file that contains statistics data to display information in chart and graph formats. File-based statistics collection is transparent to the user and increases the efficiency of transferring information. enabled
trap {source [IPv4 IPv6 Address] <name>}	Configures source IPv4 or IPv6 address or name of SNMP traps. disabled
trap-group <SNMP trap group name> [snmp-server trap <trap-name>]	Configures an SNMP trap group that stores specific traps within that group.
user	Configures an SNMPv3 user profile.
<word>	USM security model user name
[auth-prot [md5 sha] <string>]	Authentication protocol of the user and the password to use with the protocol. MD5/SHA SHA
[priv-prot {AES DES} <string>]	Privacy protocol of the user and the password to use with the protocol. AES/DES DES

Example

The following example configures an SNMP user:

```
(host) [mynode] (config) #snmp-server user temp auth-prot md5 temp12 priv-prot aes temp34
```

The following example configures an SNMP trap group:

```
(host) [mynode] (config) #snmp-server trap-group System
(host) ^[mynode] (config-submode)#snmp-server trap wlsxFlashSpaceOK
(host) ^[mynode] (config-submode)#snmp-server trap wlsxMemoryUsageOK
(host) ^[mynode] (config-submode)#snmp-server trap wlsxPowerSupplyOK
(host) ^[mynode] (config-submode)#snmp-server trap wlsxFanOK
```

Command History:

Release	Modification
ArubaOS 8.11.0.0	A new SNMP trap, wlsxLicenseThresholdLimitHit was added.
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.8.0.0	The <code>trap-group <SNMP trap group name></code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor/Mobility Conductor .

spanning-tree

```
spanning-tree
  forward-time <value>
  hello-time <value>
  max-age <value>
  mode <rapid> | <rapid-pvst>
  priority <value>
  vlan range {<word>|[remove <word> {forward-time|hello-time|max-age|priority}]}
```



RSTP is backward compatible with STP and is enabled by default. For ease of use, this command uses the spanning tree keyword.

Description

This command configures global settings for the Rapid Spanning Tree Protocol (RSTP) and Per VLAN Spanning Tree (PVST+). Refer to [interface gigabitethernet](#) for details on enabling and configuring spanning tree for an individual interface. This command configures the global RSTP settings and is backward compatible with past versions of ArubaOS using STP.

By default, all interfaces and ports run RSTP as specified in 802.1w and 802.1D. The default RSTP values can be used for most implementations.

Use the `no spanning-tree` command to disable RSTP.

Parameter	Description
<code>forward-time</code>	Specifies the time, in seconds, the port spends in the listening and learning state. During this time, the port waits to forward data packets. Range: 4-30 Default: 15 seconds
<code>hello-time</code>	Specifies the time, in seconds, between each bridge protocol data unit (BPDU) transmitted by the root bridge. Range: 1-10 Default: 2 seconds
<code>max-age</code>	Specifies the time, in seconds, the root bridge waits to receive a hello packet before changing the STP topology. Range: 6-40 Default: 20 seconds
<code>mode</code>	Set the spanning tree mode to either Rapid Spanning Tree (802.1w) or PVST+ (Per VLAN Spanning Tree)
<code><rapid></code>	Set the spanning tree mode to RSTP (Rapid Spanning Tree Protocol).

Parameter	Description
<rapid-pvst>	Set the spanning tree mode to PVST+ (Per VLAN Spanning Tree protocol)
priority	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: The highest priority bridge is the root bridge. The highest priority value is 0 (zero). Range: 0-65535 Default: 32768
vlan range <WORD>	Enter the keywords vlan range followed by the range of VLAN ID's. Separate the VLAN IDs with a hyphen, comma or both to indicate the range. For example: 2-3 or 2,4,6 or 2-6,11
remove <word>	Removes range of VLAN IDs.
remove <word> forward-time	Removes the spanning tree forward interval.
remove <word> hello-time	Removed the spanning tree hello interval.
remove <word> max-age	Removes the spanning tree maximum age interval.
remove <word> priority	Removes the spanning tree priority interval.

Examples

The following command sets the time a port spends in the listening and learning state to 3 seconds:

```
(host) [mynode] #spanning-tree forward-time 3
```

The following command sets the time the root bridge waits to transmit BPDUs to 4 seconds:

```
(host) [mynode] #spanning-tree hello-time 4
```

The following command sets the time the root bridge waits to receive a hello packet to 30 seconds:

```
(host) [mynode] #spanning-tree max-age 30
```

The following command sets the bridge priority to 10, making it more likely to become the root bridge:

```
(host) [mynode] #spanning-tree priority 10
```

The follow command sets a spanning-tree VLAN range

```
(host) [mynode] #spanning-tree vlan range 2-8,11
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Conductor.

ssh

ssh

```
disable-ciphers {aes-cbc | aes-ctr}
disable-kex
disable-mac {hmac-sha1 | hmac-sha1-96}
disable_dsa
mgmt-auth {public-key [username/password] | username/password [public-key]}
<username> <ip_addr>
```

Description

This command configures SSH access to a Mobility Conductor. Public key authentication is supported using a X.509 certificate issued to the management client. If you specify public-key authentication, you need to load the client X.509 certificate into Mobility Conductor and configure certificate authentication for the management user with the `mgmt-user ssh-pubkey` command.

The SSH authentication supports **hmac-sha1**, **hmac-sha1-96**, and **hmac-sha2-256** by default.

The `hmac-sha2-256` parameter can not be disabled.

Parameter	Description
<code>disable-ciphers</code>	Disables cipher authentication for SSH. Specify the cipher to be disabled.
<code>aes-cbc</code>	Disables AES-CBC authentication for SSH. This parameter enables the aes-ctr encryption.
<code>aes-ctr</code>	Disables AES-CTR authentication for SSH. This parameter enables the aes-cbc encryption.
<code>disable-kex</code>	Disables key exchange algorithm for SSH authentication.
<code>disable-mac</code>	Disables Message Authentication Code algorithm for SSH authentication.
<code>hmac-sha1</code>	Disables HMAC-SHA1 authentication for SSH. Starting from ArubaOS 8.6.0.5, the <code>ssh disable-mac hmac-sha1</code> command disables HMAC-SHA1 authentication and enables HMAC-SHA1-96 and HMAC-SHA2-256 authentication .

Parameter	Description
hmac-sha1-96	Disables HMAC-SHA1-96 authentication for SSH. Starting from ArubaOS 8.6.0.5, <code>ssh disable-mac hmac-sha1-96</code> command disables HMAC-SHA1-96 authentication and enables HMAC-SHA1 and HMAC-SHA2-256 authentication.
hmac-sha1 hmac-sha1-96 hmac-sha1-96 hmac-sha1	Disables HMAC-SHA1 and HMAC-SHA1-96 authentication for SSH.
disable_dsa	Disables DSA authentication for SSH. Only RSA authentication is used.
mgmt-auth	Configures the authentication method for the management user. You can specify a username and password only, public key only, or both username and password and public key.
<username>	Username for SSH login.
<ip_addr>	IPv4 or IPv6 address of the remote machine.

Example

The following command configures SSH access using public key authentication only:

```
(host) [mynode] (config) #ssh mgmt-auth public-key
mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

The following command enables **AES-CBC** and disables **AES-CTR** on the SSH server:

```
(host) [md] (config) #ssh disable-ciphers aes-ctr
```

The following command enables both the cipher encryptions on the SSH server:

```
(host) [md] (config) #no ssh disable-ciphers
```

The following command disables **HMAC-SHA1-96** on the SSH server:

```
(host) [md] (config) #ssh disable-mac hmac-sha1-96
```

The following command disables **HMAC-SHA1** and **HMAC-SHA1-96** on the SSH server:

```
(host) [md] (config) #ssh disable-mac hmac-sha1 hmac-sha1-96
```

The following command disables all **dh** key exchange algorithms on the SSH server:

```
(host) [md] (config) #ssh disable-kex dh
```

Related Commands

Command	Description
show ssh	Displays the SSH configuration details.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command modified to allow disabling key exchange algorithms. The key exchange algorithms can be disabled using the <code>disable-kex</code> parameter.
ArubaOS 8.7.0.0	Command modified to introduce SHA-2 authentication. The <code>hmac-sha1</code> and <code>hmac-sha1-96</code> parameters can be disabled using the <code>disable-mac</code> parameter.
ArubaOS 8.3.0.0	The following parameters are introduced to configure cipher and MAC authentication: <ul style="list-style-type: none">▪ <code>disable-ciphers</code>▪ <code>disable-mac</code>
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

sso idp-profile

```
sso idp-profile <sso_prof_name>  
  clone <source>  
  idp <string> <url>  
  no
```

Description

This command configures an SSO Identity Provider profile for use with application SSO with L2 Authentication. This command is used to configure an SSO IDP profile, which establishes the name and URL of the IDP server that Mobility Conductor uses for application SSO.



NOTE

ClearPass Policy Manager is the only device that can act as an IDP server for application SSO with an.

Parameter	Description
<sso_prof_name>	Name of the L2SSO profile.
clone <source>	Copies data from another SSO IDP profile.
idp <string> <url>	Configures the name and URL of Mobility Conductor's IDP server.
no	Deletes the command.

Example

```
(host) [mynode] (config) #sso idp-profile profile1  
idp url1 cppm128.arubanetworks.com/idp.login
```

Related Commands

Command	Description
show sso idp-profile	Displays all SSO IDP profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

stm

stm

```
clear-timing-stats
add-blacklist-client/add-denylist-client <macaddr>
disable-timing-stats
enable-timing-stats
kick-off-sta <macaddr> <bssid>
purge-blacklist-clients /purge-denylist-clients
purge-denylist-protected
remove-blacklist-client /remove-denylist-client <macaddr>
start-trace <macaddr>
stop-trace <macaddr>
mon-update-queue <threshold>
amon-max-batch-size <batch-size>
```

Description

This command is used to manually disconnect a client from an AP or control the denylisting of clients. If enabled, the client is not allowed to associate with any AP in the network. If the client is connected to the network when you denylist, a deauthentication message is sent to force the client to disconnect. The client is blocked for the duration specified in the virtual AP profile. The client denylist supports up to 4,000 individual client entries.

The managed device retains the client denylist in the user database, so the information is not lost if the managed device reboots. When you import or export the managed device's user database, the client denylist will be exported or imported as well.

Parameter	Description
clear-timing-stats	Clears performance monitoring stats in STM.
add-blacklist-client /add-denylist-client	MAC address of the client to be added to the denial of service list. NOTE: This parameter is available only for Managed Device.
disable-timing-stats	Disables performance monitoring in STM.
enable-timing-stats	Enables performance monitoring in STM.

Parameter	Description
kick-off-sta	When you use the kick-off-sta feature specify a client's MAC address and BSSID, the AP sends deauthorization frames to the station to disconnect it.
<macaddr>	MAC address of client to be disconnected.
<bssid>	The associated BSSID of the client to be disconnected.
purge-blacklist-client /purge-denylist-client	Clear the entire client blacklist/denylist.
purge-denylist-protected	Purge all clients from the traffic steering DoS protected list.
remove-blacklist-client/remove-denylist-client <macaddr>	Specify the MAC address of a client to remove it from the denial of service list. NOTE: This parameter is available only for Managed Device.
start-trace <macaddr>	Starts tracing probe requests and probe responses from the specified client.
stop-trace <macaddr>	Stops tracing probe requests and probe response from the specified client.
mon-update-queue <threshold>	Configures the maximum queue size for the STM monitoring updates. NOTE: This parameter is available only in Config mode on Mobility Conductor running on ArubaOS version 8.9 or earlier.

Parameter	Description
<code>amon-max-batch-size <batch-size></code>	<p>Configures the maximum number of AMONs STM will send from its queue. Any remaining AMONs in the current batch are dropped.</p> <p>NOTE: This parameter is available only in Config mode.</p>

Example

The following command blacklists/denylists a client:

```
(host) #stm add-blacklist-client /stm add-denylist-client 00:01:6C:CC:8A:6D
```

Related Commands

Command	Description
show stm	This command is used to display the deauthentication reasons and the monitoring update queue information from the station management module.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>mon-update-queue <threshold></code> parameter was deprecated.
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

support

support

Description

This command, which should be used only in conjunction with Aruba customer support, is for controller debugging purposes only. This command is used by Aruba customer support for debugging the controller. Do not use this command without the guidance of Aruba customer support.

Example

The following command allows Aruba customer support to debug the controller:

```
(host) #support
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

syscontact

syscontact <syscontact>

Description

This command configures the name of the system contact for the managed device. Use this command to enter the name of the person who acts as the system contact or administrator for the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the alphanumeric string. For example, to create the system contact name Lab Technician 1, enter "Lab Technician 1" at the prompt.

To change the existing name, enter the command with a different string. The new name takes affect immediately. To unconfigure the name, enter "" at the prompt.

Parameter	Description
<syscontact>	An alphanumeric string that specifies the name of the system contact.

Example

The following command defines **LabTechnician** as the system contact name:

```
(host) [mynode] (config) #syscontact LabTechnician
```

Related Commands

Command	Description
show syscontact	Displays the system contact information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

syslocation

syslocation <syslocation>

Description

This command configures the name of the system location for the managed device. Use this command to indicate the location of the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter "" at the prompt.

Parameter	Description
<syslocation>	An alphanumeric string that specifies the name of the system location.

Example

The following command defines **SalesLab** as the system location:

```
(host) [mynode] (config) #syslocation "Building 10, second floor, room 21E"  
syscontact LabTechnician
```

Related Commands

Command	Description
show syslocation	Displays the system location information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on managed devices.

tar

```
tar clean {crash|flash|logs} | crash [kernel] | flash | logs [tech-support {no-  
controllerip  
| user <mac-address>}]
```

Description

This command creates archive files in UNIX tar file format.

Parameter	Description
clean	Removes a tar file
crash	Removes crash.tar
flash	Removes flash.tar.gz
logs	Removes logs.tar
traces	Removes traces.tar.gz
crash	Archives the crash directory to crash.tar. A crash directory must exist.
kernel	Archives the kernel crash directory to kernel_crash.tar.
flash	Archives and compresses the /flash directory to flash.tar.gz.
logs	Archives the logs directory to log.tar.
tech-support {cluster datapath no-controllerip user <mac-address>}	Optionally, technical support information can be included in the log for a specific cluster, datapath, or no controllerip or for a specific user.
serviceability	Archives the serviceability directory to serviceability.tar.7z.
traces	Archives the traces directory to traces.tar.gz

Example

The following command creates the log.tar file with technical support information:

```
(host) [mynode] (config) #tar logs tech-support
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The <code>ipaccess-group</code> parameter requires the PEFNG license. The <code>xsec</code> parameter requires the xSec license.	Enable or config mode on Mobility Conductor.

telnet

```
telnet <host> [port <port_num>]
  cli
  soe
```

Description

This command enables telnet to Mobility Conductor or to an AP through Mobility Conductor. Use the host and port to specify the host IP address and the port to enable telnet. This command is available only in **Enable** mode.

Use the **cli** option to enable telnet to Mobility Conductor.

Use the **soe** option to enable telnet using the SoE protocol. This allows you to remotely manage an AP directly connected to Mobility Conductor.

Parameter	Description
host	IP address of the host Mobility Conductor
port	Port number in the host
cli	Enable telnet using the CLI. Disabled
soe	Enable telnet using Serial over Ethernet (SoE). Disabled

Example

The following example enables telnet to Mobility Conductor using the CLI:

```
(host) [mynode] (config) #telnet cli
```

Related Commands

Command	Description
show telnet	Displays the telnet access status.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

test

```
test jitter <probe_ip> <src_intf> <burst_count>
```

Description

This command enables jitter measurement for a specific IP address.

Parameter	Description
jitter	Test jitter probes (udp).
<probe_ip>	Specify IP address for which jitter is to be measured.
<src_intf>	Specify source interface VLAN.
<burst_count>	Specify the number of probes to be sent. 1-4000

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

threshold

```
threshold
  controlpath-cpu <value>
  controlpath-memory <value>
  datapath-cpu <value>
  no-of-APs <value>
  no-of-locals <value>
  no-of-vaps <value>
  total-tunnel-capacity <value>
  user-capacity <value>
no
```

Description

This command configures managed device capacity thresholds which, when exceeded, trigger alerts. The managed device sends a *wlsxThresholdExceeded* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdCleared* SNMP trap and error message will be triggered if the resource usage drops below the threshold once again.

Parameter	Description
<code>controlpath-cpu <value></code>	Sets an alert threshold, in percentage, for the control path CPU capacity that must be exceeded before the alert is sent. Range: 0-100% Default: 80%
<code>controlpath-memory <value></code>	Sets an alert threshold, in percentage, for the control path memory consumption that must be exceeded before the alert is sent. Range: 0-100% Default: 85%
<code>datapath-cpu <value></code>	Sets an alert threshold, in percentage, for the datapath CPU capacity that must be exceeded before the alert is sent. Range: 0-100% Default: 30%
<code>no-of-APs <value></code>	The maximum number of APs that can be connected to a managed device is determined by that managed device's model type and installed licenses. Use this command to trigger an alert when the number of APs currently connected to the managed device exceeds a specific percentage of its total AP capacity. Range: 0-100% Default: 80%

Parameter	Description
<code>no-of-locals <value></code>	Sets an alert threshold, in percentage, for the Mobility Conductor's capacity to support managed devices that must be exceeded before the alert is sent. Range: 0-100% Default: 80%
<code>no-of-vaps <value></code>	The maximum number of Virtual APs that can be connected to a managed device is determined by that managed device's model type and installed licenses. Use this command to trigger an alert when the number of Virtual APs currently connected to the managed device exceeds a specific percentage of its total AP capacity. Range: 0-100% Default: 80%
<code>total-tunnel-capacity <value></code>	Sets an alert threshold, in percentage, for the managed device's tunnel capacity that must be exceeded before the alert is sent. Range: 0-100% Default: 80%
<code>user-capacity <value></code>	Sets an alert threshold, in percentage, for the managed device's user capacity that must be exceeded before the alert is sent. Range: 0-100% Default: 80%

Example

The following command configures a new alert threshold for controlpath memory consumption:

```
(host) [mynode] (config) #threshold datapath-cpu 90
```

If this threshold is exceeded then subsequently drops below the 90% threshold, the managed device would send the following two syslog error messages.

```
Mar 10 13:13:58 nanny[1393]: <399816> <ERRS> |nanny| Resource 'Control-Path Memory' has gone above 90% threshold, value : 93
Mar 10 13:16:58 nanny[1393]: <399816> <ERRS> |nanny| Resource 'Control-Path Memory' has come below 90% threshold, value : 87
```

Related Commands

Command	Description
show threshold	Displays the managed device capacity thresholds which, when exceeded, triggers alerts.

Command History

Release	Modification
ArubaOS 8.6.0.0	The <code>no-of-vaps<value></code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

time-range

```
time-range
  absolute <name> [end <mm/dd/yyyy> <hh:mm>] [start <mm/dd/yyyy> <hh:mm>]
  no
  periodic <name>
    Daily <hh:mm> to <hh:mm>
    Friday <hh:mm> to <hh:mm>
    Monday <hh:mm> to <hh:mm>
    Saturday <hh:mm> to <hh:mm>
    Sunday <hh:mm> to <hh:mm>
    Thursday <hh:mm> to <hh:mm>
    Tuesday <hh:mm> to <hh:mm>
    Wednesday <hh:mm> to <hh:mm>
    Weekday <hh:mm> to <hh:mm>
    Weekend <hh:mm> to <hh:mm>
```

Description

This command configures time ranges. You can use time ranges when configuring session ACLs. Once you configure a time range, you can use it in multiple session ACLs.

Parameter	Description
<code>absolute <name></code>	Specifies an absolute time range, with a specific start time, end time, and date.
<code>end <mm/dd/yyyy> <hh:mm></code>	Specifies the end time of the time range.
<code>start <mm/dd/yyyy> <hh:mm></code>	Specifies the start time of the time range.
<code>no</code>	Negates any configured parameter.
<code>periodic <name></code>	Specifies a recurring time range. Select the day of the week occurrence, the start time (hh:mm), and the end time (hh:mm).

Example

The following command configures a time range for daytime working hours:

```
(host) [mynode] (config) #time-range periodic working-hours
weekday 7:30 to 18:00
```

Related Commands

Command	Description
show time-range	Displays the configured time ranges.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license.	Enable and Config modes on Mobility Conductor and managed devices.

time-range-profile

```
time-range-profile <profile-name>  
  absolute [start-date <abs_sdate> start-time <abs_stime>][end-date <abs_edate>  
  end-time <abs_etime>]  
  clone  
  mode {absolute|periodic}  
  no
```

Description

This command configures time range profiles. You can use time range profiles when configuring session ACLs. After you configure a time range profile, you can use it in multiple session ACLs.

Parameter	Description
<profile-name>	Name of the time range profile.
absolute	Specifies an absolute time range profile, with a specific start date, start time, end date, and end time.
start-date <abs_sdate>	Start date for the time range profile (mm/dd/yyyy).
start-time <abs_stime>	Start time for the time range profile (hh:mm).
end-date <abs_edate>	End date for the time range profile (mm/dd/yyyy).
end-time <abs_etime>	End time for the time range profile (hh:mm).
clone	Copy data from another time range profile.
mode	Time range profile mode: <ul style="list-style-type: none">▪ Absolute▪ Periodic
no	Negates any configured parameter.

Example

The following command configures a time range profile for a training class that takes place between 8:30AM and 6:00PM:

```
(host) [node] (config) #time-range-profile training absolute  
start-date <06/19/2016>  
start-time <08:30>  
end-date <06/19/2016>  
end-time <18:00>
```

Related Commands

Command	Description
show time-range	Displays the configured time ranges.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license.	Enable and Config modes on Mobility Conductor and managed devices.

tm

```
tm mon update-queue <threshold>
```

Description

This command is used to configure the maximum queue size for the TM monitoring updates.

Parameter	Description
mon update-queue <threshold>	Configures the maximum queue size for the TM monitoring updates.

Example

The following command configures the maximum queue size for the TM monitoring updates.

```
(host) #tm mon update-queue 5000
```

Related Commands

Command	Description
show tm	This command is used to display the monitoring update queue information of the telemetry manager module.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

tm trace

```
tm trace
  filter {category|ip-addr <ip-addr>|mac <mac>}
  loglevel
```

Description

This command is used to configure the TM traces.

Parameter	Description
filter	Specify the filter to use for the trace.
category	Specify one of the following trace category to enable or disable: <ul style="list-style-type: none">▪ all: Traces all events.▪ amon: Traces AMON events.▪ cli: Traces CLI events.▪ db_info: Traces internal DB info events.▪ db_stats: Traces internal DB stats events.▪ gsm: Traces GSM events.▪ mon: Traces MON events.▪ papi: Traces PAPI events.▪ syslog: Traces Syslog events.
ip-addr <ip-addr>	Trace only events for this IP address.
mac <mac>	Trace only events for this MAC address (contextual)
loglevel	Specify one of the following loglevel of syslogs that will be included in the trace: <ul style="list-style-type: none">▪ alert: Trace all logs equal or higher than LOG_ALERT▪ critical: Trace all logs equal or higher than LOG_CRIT▪ debug: Trace all logs equal or higher than LOG_DEBUG▪ emergency: Trace all logs equal or higher than LOG_EMERG▪ error: Trace all logs equal or higher than LOG_ERR▪ info: Trace all logs equal or higher than LOG_INFO▪ notice: Trace all logs equal or higher than LOG_NOTICE▪ warn: Trace all logs equal or higher than LOG_WARN

Example

The following command configures the maximum queue size for the TM monitoring updates.

```
(host) #tm mon update-queue 5000
```

Related Commands

Command	Description
show tm	This command is used to display the monitoring update queue information of the telemetry manager module.

Command History

Release	Modification
ArubaOS 8.10.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

traceoptions

```
traceoptions
  chassis-manager flags {all|association|debug|environment-
monitoring|fru|interface|interface-statistics|ipc|poe-configuration|poe-
statistics|statistics-sync|system-statistics}
  igmp flags {all|debug|leave|query|report}
  igmp-snooping flags {all|config|errors|receive|transmit}
  interface-manager {flags {all|configuration|dhcp-
client|ethernet|infrastructure|lacp|loopback|mgmt|oam|port-channel|port-
mirroring|system-information|tunnel|vlan} | level {debug|error|verbose}}
  layer2-forwarding {flags{all|config|fdb|hsl|interface|ipc|learning|nexthop|port-
loop-protect|sysinfo|task|timer|tunneled-node|vlan|vlan-assignment|vlan-port} |
level{debugging|errors|informational} |
{size <tracefile_size>}}
  lldp flags {all|errors|receive|system-state|transmit}
  mstp {flags {all|config|debug|port-information|received-bpdu-all|role-
selection|sent-bpdu-all|state-machine-changes|system|topology-change|} |
port<mstp_trace_port>}
  no
  ospf flags {all|cnf|db|dd|debug|dr-elec|flood|hello|lsa|lsr|lsu|msm|pkt-
all|spf|state}
  pim flags {adjacency|all|debug|jp-asserts|register|route|state}
  rmon {flags {alarm|all|cli|event|history|ifstat|log|snmp} | {level
{alert|critical|debugging|emergency|errors|informational|notice|warning} | size
<trace_file_ize>}}
  routing flags {all|arp|configuration|event|interface|route}
  stack-manager {flags {adjacency|all|asp|configuration|primary-
election|route|system} | level
{alert|critical|debugging|emergency|errors|informational|notice|warning}}
```

Description

This command configures the traceoptions to monitor and log traffic flows.

Parameter	Description
chassis-manager flags	Configures the chassis manager trace options: <ul style="list-style-type: none">▪ all—Enables all chassis manager debug tracing.▪ association—Enables stack membership and association tracing.▪ debug—Enables generic chassis manager debug tracing.▪ environment-monitoring—Enables environment monitor debug tracing.▪ fru— Enables FRU reporting and management tracing.▪ interface—Enables interface debug tracing.

Parameter	Description
	<ul style="list-style-type: none"> ▪ interface-statistics—Enables packet statistics on interface tracing. ▪ ipc—Enables inter-process message exchange tracing. ▪ poe-configuration—Enables power-over-ethernet configuration tracing. ▪ poe-statistics—Enables power-over-ethernet statistics tracing. ▪ statistics-sync—Enables statistics tracing. ▪ system-statistics—Enables chassis system statistics tracing.
igmp flags	<p>Configures the IGMP trace options:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing on all IGMP modules. ▪ debug—Enables internal state tracing for IGMP modules. ▪ leave—Enables IGMP leave processing tracing. ▪ query—Enables IGMP query processing tracing. ▪ report—Enables IGMP report processing tracing.
igmp-snooping flags	<p>Configures the IGMP snooping trace options:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing on all igmp-snooping modules. ▪ config—Enables igmp-snooping configuration tracing. ▪ errors— Enables igmp-snooping error tracing. ▪ receive—Enables igmp-snooping PDU received (RX) tracing. ▪ transmit—Enables igmp-snooping PDU transmit (TX) tracing.
interface-manager {flags level}	<p>Configures the interface manager trace flags:</p> <ul style="list-style-type: none"> ▪ all—Enables all interface manager debug message tracing. ▪ configuration—Enables configuration debug tracing. ▪ dhcp-client—Enables dhcp client debug tracing. ▪ ethernet—Enables ethernet interface debug tracing. ▪ infrastructure—Enables infrastructure debug tracing. ▪ lACP—Enables LACP debug tracing. ▪ loopback—Enables loopback interface debug tracing.

Parameter	Description
	<ul style="list-style-type: none"> ▪ mgmt—Enables management interface debug tracing. ▪ oam—Enables OAM debug tracing. ▪ port-channel—Enables port-channel debug tracing. ▪ port-mirroring—Enables port mirroring debug tracing. ▪ system-information—Enables system debug messages tracing. ▪ tunnel—Enables tunnel interface debug tracing. ▪ vlan—Enables vlan interface debug tracing. <p>Configures the level for interface manager tracing:</p> <ul style="list-style-type: none"> ▪ debug—Debug messages ▪ error—Error messages ▪ verbose—Verbose debug messages
<pre>layer2-forwarding {flags level size}</pre>	<p>Configures the layer2 forwarding trace flags:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing on all switching modules. ▪ config—Enables config module tracing. ▪ fdb—Enables forwarding database module tracing. ▪ hsl—Enables HSL module tracing. ▪ interface—Enables interface module tracing. ▪ ipc—Enables IPC tracing. ▪ learning—Enables learning module tracing. ▪ nexthop—Enables nexthop module tracing. ▪ port-loop—Enables Port loop protect Protocol tracing. ▪ sysinfo—Enables sysinfo module tracing. ▪ task—Enables task tracing. ▪ timer—Enables task timer tracing. ▪ tunneled-node—Enables tunneled-node module tracing. ▪ vlan—Enables vlan module tracing. ▪ vlan-assignment—Enables VLAN assignment module tracing. ▪ vlan-port—Enables VLAN port module tracing. <p>Configures the layer2 forwarding tracing levels:</p> <ul style="list-style-type: none"> ▪ debug—Debug messages ▪ error—Error messages ▪ informational—Informational messages <p>Configures the maximum size for layer2 forwarding trace file in MB.</p>
<pre>lldp flags</pre>	<p>Configures the LLDP trace options:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ all—Enables tracing on all lldp modules. ▪ errors—Enables lldp error tracing. ▪ receive—Enables lldp PDU receive (RX) tracing. ▪ system-state—Enables lldp system-state tracing. ▪ transmit—Enables lldp PDU transmit (TX) tracing.
<pre>mstp {flags port}</pre>	<p>Configures the MSTP trace flags and trace port:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing on all mstp modules ▪ config—Enables mstp config tracing. ▪ debug—Enables mstp debug tracing. ▪ port-information—Enables mstp port information tracing. ▪ received-bpdu-all—Enables mstp received bpdu tracing. ▪ role-selection—Enables mstp role selection tracing. ▪ sent-bpdu-all—Enables mstp sent bpdu tracing. ▪ state-machine-changes—Enables mstp state machine change tracing. ▪ system—Enables mstp system tracing. ▪ topology-change—Enables mstp topology change tracing.
<pre>ospf flags</pre>	<p>Configures the OSPF trace options:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing for all ospf events. ▪ cnf—Enables configuration events tracing. ▪ db—Enables database operations tracing. ▪ dd—Enables database description packets tracing. ▪ debug—Enables internal debug tracing. ▪ dr-elect—Enables designated router election tracing. ▪ flood—Enables linkstate flooding tracing. ▪ hello—Enables tracing for hello packets. ▪ lsa—Enables link state advertisement packets tracing. ▪ lsr—Enables link state request packets tracing. ▪ lsu—Enables link state update packets tracing. ▪ msm—Enables msm events tracing. ▪ pkt-all—Enables tracing for all packets. ▪ spf—Enables SPF operations tracing. ▪ state—Enables interface, neighbor, area changes tracing.

Parameter	Description
<p>pim flags</p>	<p>Configures PIM sparse mode trace options:</p> <ul style="list-style-type: none"> ▪ adjacency—Enables pim sparse mode adjacency tracing. ▪ all—Enables tracing on all pim sparse mode modules. ▪ debug—Enables internal state tracing for pim sparse mode modules. ▪ jp-asserts—Enables pim sparse mode join-prune/assert tracing. ▪ register—Enables pim sparse mode register tracing. ▪ route—Enables pim sparse mode route tracing. ▪ state—Enables pim sparse mode state tracing.
<p>rmon {flags level size}</p>	<p>Configures the RMON trace flags:</p> <ul style="list-style-type: none"> ▪ alarm—Enables rmon alarm module debug tracing. ▪ all—Enables rmon all module debug tracing. ▪ cli—Enables rmon CLI module debug tracing. ▪ event—Enables rmon event debug tracing. ▪ history—Enables rmon history module debug tracing. ▪ ifstat—Enables rmon interface statistics debug tracing. ▪ log—Enables rmon log debug tracing. ▪ snmp—Enables rmon SNMP module debug tracing. <p>Configures the RMON tracing levels:</p> <ul style="list-style-type: none"> ▪ alert—Alert messages ▪ critical—Critical messages ▪ debugging—Debug messages ▪ emergency—Emergency messages ▪ errors—Error messages ▪ informational—Informational messages ▪ notice—Notification messages ▪ warning—Warning messages <p>Configures the maximum size for RMON trace file in MB.</p>
<p>routing flags</p>	<p>Configures the layer3 manager trace options:</p> <ul style="list-style-type: none"> ▪ all—Enables tracing on all layer3 manager events. ▪ arp—Enables arp module tracing. ▪ configuration—Enables layer3 configuration processing tracing.

Parameter	Description
	<ul style="list-style-type: none"> ▪ event—Enables layer3 manager system events tracing. ▪ interface—Enables layer3 manager interface events tracing. ▪ route—Enables route table updates tracing.
<pre>stack-manager {flags level}</pre>	<p>Configures the stack manager trace flags:</p> <ul style="list-style-type: none"> ▪ adjacency—Enables stack-manager adjacency tracing. ▪ all—Enables tracing for all stack-manager modules. ▪ asp—Enables aruba stacking protocol tracing. ▪ configuration—Enables tracing for configuration of stack-manager. ▪ primary-election—Enables tracing for primary election. ▪ route—Enables stack-manager route calculations tracing. ▪ system—Enables tracing for stack-manager interaction with other components. ▪ webui—Enables tracing for stack-manager interaction with WebUI. <p>Configures the stack manager tracing level:</p> <ul style="list-style-type: none"> ▪ alert—Alert messages ▪ critical—Critical messages ▪ debugging—Debug messages ▪ emergency—Emergency messages ▪ errors—Error messages ▪ informational—Informational messages ▪ notice—Notification messages ▪ warning—Warning messages

Example

The following command enables tracing on all IGMP modules:

```
(host) [mynode] (config) #traceoptions igmp flags all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

tracepath

tracepath <global-address>

Description

Traces the path of an IPv6 host and identifies points of failure in your IPv6 network.

Parameter	Description
<global-address>	The IPv6 global address of the host.

Example

The following command traces the path of the specified IPv6 host.

```
(host) [mynode] (config) #tracepath 2005:d81f:f9f0:1001::14
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

traceroute

```
traceroute <ipaddr>  
  source
```

Description

Trace the route to the specified IP address.

Syntax

Parameter	Description
<ipaddr>	The destination IP address.
source <ipaddr>	Sets the source IP address through which packets are sent for tracing route.

Usage Guidelines

Use this command to identify points of failure in your network.

Example

The following command traces the route to the device identified by the IP address 10.1.2.3.

```
(host) [mynode] (config) #traceroute 10.1.2.3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

tunnel-group

```
tunnel-group <tungrpname>  
  mode {l2|l3}  
  no  
  preemptive-failover  
  tunnel <tunnel-id>
```

Description

This command creates a tunnel-group to group a set of tunnels. Use this command to provide redundancy for L3 GRE tunnels. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down.

To enable L3 GRE tunnel group, you must:

- Configure a tunnel-group to group a set of tunnels.
- Enable tunnel keepalives on all the tunnel interfaces assigned to the tunnel-group, and
- Configure the session ACL with the tunnel-group as the redirect destination.

To enable L2 GRE tunnel group, you must:

- Configure the member tunnel and add them to the appropriate VLAN.
- Enable tunnel keepalives on the tunnel interface.
- Configure the tunnel-group and set the group type to L2, and
- Add the member tunnel to the group



You can configure up to 32 tunnel-groups on a with a maximum of 5 tunnels in each tunnel-group.

Parameter	Description
mode {l2 l3}	Set the type of tunnel-group. Default: l3
no	Negates any parameter configured.
preemptive-failover	When enabled, this option automatically redirects the traffic upon detecting an active tunnel with a higher precedence in the tunnel-group. When disabled, the traffic gets redirected to a higher precedence tunnel only when the tunnel carrying the traffic fails. Default: Enabled
tunnel <tunnel-id>	Adds the specified tunnel ID to the tunnel group. Range: 1-16777215.

Example

The following set of commands create a tunnel-group with tunnel IDs 10 and 20 as the members:

```
(host) [mynode] (config) #tunnel-group tgroup1
(host) [mynode] (config-tunnel-group) # mode 13
(host) [mynode] (config-tunnel-group) # tunnel 10
(host) [mynode] (config-tunnel-group) # tunnel 20
(host) [mynode] (config-tunnel-group) #preemptive-failover
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

tunnel-loop-prevention

tunnel-loop-prevention

Description

This command prevents prevent forwarding loops between tunneled nodes on the managed device.

To allow a tunneled node-connected machine to communicate with another managed device that is a connected client on the same subnet, you must enable **ip local-proxy-arp**.

Example

The following command prevents tunneled node forwarding:

```
(host) [mynode] (config) #tunnel-loop-prevention
```

Related Commands

Command	Description
show tunneled-node	Displays the wired tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

tunneled-node-address

tunneled-node-address <tnode-ip-address>

Description

This command configures the IP address of a tunneled node server. An Aruba managed device can operate as a Wi-Fi managed device, terminating GRE tunnels from tunneled node switches. As a Wi-Fi managed device, the managed device does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as tunneled node ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central managed device for processing.

Parameter	Description
<tnode-ip-address>	IP address of the managed device. This is the loopback or IP address of the managed device acting as a tunneled node managed device.

Example

The following command configures the address of a managed device for tunneled nodes:

```
(host) [mynode] (config) #tunneled-node-address 192.168.1.245
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

tunnel-node-mtu

tunnel-node-mtu <mtu>

Description

This command configures the MTU of a tunneled node. An Aruba managed device can operate as a Wi-Fi managed device, terminating GRE tunnels from tunneled node switches. As a Wi-Fi managed device, the managed device does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as tunneled node ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central managed device for processing.



This command does not take effect when the tunnel node client is an switch.

Parameter	Description
tnode-mtu	Value of the MTU for the tunneled nodes Range: 1024 to 9216

Example

The following command configures the MTU of a managed device for tunneled nodes:

```
(host) [mynode] (config) #tunnel-node-mtu 1030
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

uap-blacklist / uap-denylist

```
uap-blacklist / uap-denylist
  add mac-address <address> description <description>
  del mac-address <address>
  modify mac-address <address> description <description>
  purge
```

Description

This command configures a Unified AP (UAP) blacklist/denylist database entry. You can add, delete, or modify AP MAC addresses and description to the database. If you enable the blacklist/denylist policy in the AP deploy profile, the policy is applied to the APs included in this list. You can also purge this database from the device.

Parameter	Description
<code>add mac-address <address> description <description></code>	Adds the specified AP MAC address to the blacklist/denylist database.
<code>del mac-address <address></code>	Deletes the specified AP MAC address from the blacklist/denylist database.
<code>modify mac-address <address> description <description></code>	Modifies the details of an existing MAC address entry in the blacklist/denylist database.
<code>purge</code>	Purges the blacklist/denylist database.

Example

The following command adds the 11:11:11:11:11:11 MAC address entry to the UAP blacklist/denylist database:

```
(host) [mynode] #uap-blacklist / uap-denylist add mac-address
11:11:11:11:11:11 description AP-203H
The following command modifies the description of the 11:11:11:11:11:11 MAC
address entry from AP-203H to AP-203R in the UAP blacklist/denylist
database:
```

Related Commands

Command	Description
ap deploy-profile	The blacklist/denylist policy when enabled in the AP deploy profile, applies the policy to the UAP blacklist/denylist database entries.
show uap-blacklist/show uap-denylist	This command displays the UAP blacklist/denylist database entries.

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>blacklist</code> have been replaced with <code>denylist</code> .
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

UCC

```
ucc
  custom-sip
    app-name
    custom_sip_port
    enable
    key
    no
    priority {video <0-63>|voice <0-63>}
  facetime {enable|no|priority video <0-63>}
  h323 {enable|no|priority voice <0-63>}
  ich {channel-utilization-threshold <50-95>|enable|no}
  jabber
    enable
    no
    priority {app-sharing <0-63>|video <0-63>|voice <0-63>}
    server-ip <server-ip>
  noe {enable|no|priority voice <0-63>}
  rtpa-config {enable|no|upstream}
  sccp {enable|no|priority voice <0-63>}
  session-idle-timeout {no|value <35-250>}
  sip
    enable
    midcall-req-timeout
    no
    priority {video <0-63>|voice <0-63>}
    rtcp-inactivity
  skype4b
    enable
    no
    priority {app-sharing <0-63>|video <0-63>|voice <0-63>}
    sdn {http|https}
  teams
  vocera {enable|no|priority voice <0-63>}
  webrtc
    enable
    no
    priority {video <0-63>|voice <0-63>}
  wificalling
    dns-pattern <dns-pattern> service-provider <service-provider>
    enable
    no
    priority voice <0-62>
```

Description

This command configures the various UCC Application Layer Gateways (ALGs). The UCC ALGs must be configured from the **/mm** node hierarchy of Mobility Conductor. All the ALGs are enabled by default.

Parameter	Description
custom-sip	<p>Configures the custom SIP ALG. The ALG is enabled by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ app-name - Configure an application name. ▪ custom_sip_port - Configure the custom SIP port number. ▪ enable - Enable the custom SIP ALG. ▪ key - Configure the user-agent key-name. ▪ no - Remove or negate a parameter. ▪ priority- Configure the DSCP value for the video or voice session. <p>Range: Priority voice: 0-63 and priority video: 0-63</p>
facetime	<p>Configures the Apple® FaceTime ALG. The ALG is enabled by default. The DSCP value for the video session is 34 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ enable- Enable the Apple Facetime ALG on the Mobility Conductor. ▪ no- Remove or negate a parameter. ▪ priority- The DSCP value for the video session. <p>Range: Priority video: 0-63 Default: Priority video: 34</p>
h323	<p>Configures the H.323 ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ enable- Enable the H.323 ALG on the Mobility Conductor. ▪ no- Remove or negate a parameter. ▪ priority- The DSCP value for the voice session. <p>Range: Priority voice: 0-63 Default: Priority voice: 46</p>
ich	<p>Configures the intelligent call handling. The setting is enabled by default. The Channel Utilization Threshold is 90 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ channel-utilization-threshold-The maximum limit for the channel utilization. ▪ enable-Enable intelligent call handling on the Mobility Conductor. ▪ no-Remove or negate a parameter. <p>Range: Channel-utilization-threshold: 50-95 Default: Channel-utilization-threshold: 90</p>

Parameter	Description
jabber	<p>Configures the Cisco® Jabber ALG. The ALG is enabled by default. Enter the Cisco Unified Communication Manager IM & Presence server IP. The DSCP values for the voice, video, and app-sharing sessions are 46, 34, and 34, respectively, by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>–Enable Jabber ALG on the Mobility Conductor. ▪ <code>no</code>–Remove or negate a parameter. ▪ <code>priority</code>–The DSCP value for voice, video, and app-sharing sessions. ▪ <code>server-ip</code>–Jabber server IP. <p>Range: App-sharing, video, and voice: 0-63 Default: App-sharing: 34, video: 34, and voice: 46</p>
noe	<p>Configures the Alcatel-Lucent® New Office Environment (NOE) ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>– Enable the NOE ALG on the Mobility Conductor. ▪ <code>no</code>– Remove or negate a parameter. ▪ <code>priority</code>– The DSCP value for the voice session. <p>Range: Priority voice: 0-63 Default: Priority voice: 46</p>
rtpa-config	<p>Configures the real-time analysis of VoIP calls including upstream real-time analysis. The setting is enabled by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>– Enable Real-Time Analysis of VoIP calls. ▪ <code>no</code>– Remove or negate a parameter. ▪ <code>upstream</code>–Enable upstream Real-Time Analysis of VoIP calls.
sccp	<p>Configures the Cisco Skinny Client Control Protocol (SCCP) ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>– Enable the SCCP ALG on the Mobility Conductor. ▪ <code>no</code>– Remove or negate a parameter. ▪ <code>priority</code>– The DSCP value for the voice session. <p>Range: Priority voice: 0-63 Default: Priority voice: 46</p>
session-idle-timeout	<p>Configures the UCC session idle timeout. On configuring this parameter, if the voice session is idle for the configured period, UCM aborts the session on the managed device due to inactivity. The default value is 35. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>no</code>– Remove or negate a parameter.

Parameter	Description
	<ul style="list-style-type: none"> ▪ <code>value</code>- Configure UCC session idle timeout in seconds. <p>Range: Value: 35-250 Default: Value: 35</p>
sip	<p>Configures the Session Initiation Protocol (SIP) ALG. The ALG is enabled by default. You can enable the SIP Midcall request timeout and RTCP inactivity settings. The DSCP values for the voice and video sessions are 46 and 34, respectively, by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>-Enable SIP ALG on the Mobility Conductor. ▪ <code>midcall-req-timeout</code>-Enable SIP Midcall request timeout. ▪ <code>no</code>-Remove or negate a parameter. ▪ <code>priority</code>-The DSCP value for voice and video sessions. ▪ <code>rtcp-inactivity</code>-Enable Real-Time Control Protocol inactivity. <p>Range: Video and voice: 0-63 Default: Video: 34 and voice: 46</p>
skype4b	<p>Configures the Microsoft® Lync/Skype for Business ALG. The ALG is enabled by default. You can set the Skype for Business SDN listen protocol over HTTP or HTTPS. Based on the SDN listen protocol configuration, Mobility Conductor accepts either HTTP or HTTPS messages from the Skype for Business SDN manager. The DSCP values for the voice, video, and app-sharing sessions are 46, 34, and 34, respectively, by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ <code>enable</code>-Enable Skype for Business ALG on the Mobility Conductor. ▪ <code>no</code>-Remove or negate a parameter. ▪ <code>priority</code>-The DSCP value for voice, video, and app-sharing sessions. ▪ <code>sdn</code>-Skype for Business SDN listen protocol. The default Skype for Business SDN API listen port is 32000. <p>Range: app-sharing, video, and voice: 0-63 Default: app-sharing: 34, video: 34, and voice: 46</p>
teams	<p>Configure the Microsoft Teams ALG. The ALG is enabled by default.</p> <ul style="list-style-type: none"> ▪ <code>enable</code>-Enable the Microsoft Teams ALG on the Mobility Conductor. ▪ <code>no</code>-Remove or negate a parameter. ▪ <code>priority</code>-The DSCP value for video and voice.

Parameter	Description
vocera	<p>Configure the Vocera ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ enable- Enable the Vocera ALG on the Mobility Conductor. ▪ no- Remove or negate a parameter. ▪ priority- The DSCP value for the voice session. <p>Range: Priority voice: 0-63 Default: Priority voice: 46</p>
webrtc	<p>Configure the WebRTC ALG. The ALG is enabled by default. This parameter has the following sub-parameters:</p> <ul style="list-style-type: none"> ▪ enable- Enable the WebRTC ALG on the Mobility Conductor. ▪ no- Remove or negate a parameter. ▪ priority- The DSCP value for the video or voice session. <p>Range: Priority video: 0-63 priority voice: 0-63 Default: Priority voice: 46</p>
wificalling	<p>Configures the Wi-Fi Calling. Wi-Fi Calling is enabled by default. The DSCP value for the voice session is 46 by default.</p> <ul style="list-style-type: none"> ▪ dns-pattern- Configure the DNS pattern for the carrier. A maximum of 10 DNS patterns can be configured. DNS patterns for known carriers are configured by default. Default built-in patterns are: <ul style="list-style-type: none"> - 3 HK - wlan.three.com.hk - ATT - epdg.epc.att.net - Rogers - epdg.epc.mnc720.mcc302.pub.3gppnetwork.org - SmarTone - epdg.epc.mnc006.mcc454.pub.3gppnetwork.org - Sprint - primgw.vowifi2.spcsdns.net - T-Mobile - ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org - Verizon - wo.vzww.com <p>If the ePDG FQDN of the carrier does not match with the default patterns, use this option to configure the DNS pattern for the carrier.</p> <p>NOTE: The DNS IP address that Mobility Conductor learns for Wi-Fi Calling age out automatically, if there was no DNS query or response matching that IP for more than seven days.</p> ▪ service-provider- Add the service provider name for enhanced visibility. ▪ enable- Enable the Wi-Fi calling ALG on the Mobility Conductor. ▪ no- Remove or negate a parameter.

Parameter	Description
	<ul style="list-style-type: none"> ▪ priority- The DSCP value for the voice session. Range: Priority voice: 0-62 Default: Priority voice: 46

Examples

The following commands enables Wi-Fi calling on Mobility Conductor:

```
(host) [mm] (config) #ucc wificalling
(host) ^[mm] (WiFiCalling Configuration) #enable
The following command displays the UCC client MAC and IP address table. The
ucc tables command should be executed from the enable mode:
(host) [mynode] #ucc tables
-----
UCC Client MAC table
-----
Client (MAC)      Client (IP)      Type      ALG
-----
68:17:29:9f:b6:77  10.15.88.234    Client    Jabber/xmpp/SIP
-----
UCC Client IP table
-----
Client (MAC)      Client (IP)      Type      ALG
-----
00:0b:86:8f:d6:b7  10.15.16.50     Server    SIP
00:0b:86:8f:d6:b7  10.15.16.30     Server    Jabber
68:17:29:9f:b6:77  10.15.88.234    Client    Jabber/xmpp/SIP
-----
```

Related Commands

Command	Description
show ucc call-info cdrs	This command displays the Call Detailed Records (CDR) statistics for UCC.
show ucc client-info	This command displays the UCC client status and CDR statistics.
show ucc custom-sip	This command displays the custom SIP ALG configuration.
show ucc dns-ip-learning	This command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device. This command is specific for Wi-Fi calling clients.
show ucc facetime	This command displays the Apple Facetime ALG configuration.

Command	Description
<u>show ucc h323</u>	This command displays the H.323 ALG configuration.
<u>show ucc ich</u>	This command displays the Intelligent Call Handling configuration.
<u>show ucc internal-state</u>	This command displays the number of CDRs, flows, and voice clients created. This is a debug command.
<u>show ucc jabber</u>	This command displays the Cisco Jabber ALG configuration.
<u>show ucc noe</u>	This command displays the Alcatel-Lucent New Office Environment (NOE) ALG configuration.
<u>show ucc rtpa-config</u>	This command displays the real-time analysis configuration.
<u>show ucc rtpa-report</u>	This command displays the real-time analysis report.
<u>show ucc sccp</u>	This command displays the Cisco Skinny Client Control Protocol (SCCP) ALG configuration.
<u>show ucc session-idle-timeout</u>	This command displays the UCC session idle timeout configuration.
<u>show ucc sip</u>	This command displays the SIP ALG configuration.
<u>show ucc skype4b</u>	This command displays the Skype4B ALG configuration.
<u>show ucc statistics</u>	This command displays the UCC call statistics.
<u>show ucc teams</u>	This command displays the Microsoft Teams ALG configuration.
<u>show ucc trace-buffer</u>	This command displays the UCC call message trace buffer for Cisco Jabber, Cisco SCCP, SIP, and Microsoft Skype for Business ALGs.
<u>show ucc vocera</u>	This command displays the Vocera ALG configuration.
<u>show ucc webrtc</u>	This command displays the webRTC ALG configuration.
<u>show ucc wificalling</u>	This command displays the Wi-Fi calling configuration.

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>teams</code> parameter is introduced.

Release	Modification
ArubaOS 8.6.0.0	The <code>custom-sip</code> and <code>webrtc</code> parameters are introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license.	Config mode on Mobility Conductor.

upgrade internal

```
upgrade internal managed-devices
  copy configured-fileserver
    file <img-file> list <mac-list> partition {0|1}
    force-file <img-file-forced> list <mac-list> partition {0|1}
    force-version <img-version-forced> list <mac-list> partition {0|1}
    version <img-version> list <mac-list> partition {0|1}
  copy fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost>
<username> <image-path>|tftp <imagehost> <image-path>}
    file <img-file> list <mac-list> partition {0|1}
    force-file <img-file-forced> list <mac-list> partition {0|1}
    force-version <img-version-forced> list <mac-list> partition {0|1}
    version <img-version> list <mac-list> partition {0|1}
  copy-reboot configured-fileserver
    file <img-file> list <mac-list> partition {0|1}
    force-file <img-file-forced> list <mac-list> partition {0|1}
    force-version <img-version-forced> list <mac-list> partition {0|1}
    version <img-version> list <mac-list> partition {0|1}
  copy-reboot fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost>
<username> <image-path>|tftp <imagehost> <image-path>}
    file <img-file> list <mac-list> partition {0|1}
    force-file <img-file-forced> list <mac-list> partition {0|1}
    force-version <img-version-forced> list <mac-list> partition {0|1}
    version <img-version> list <mac-list> partition {0|1}
  reboot list <mac-list>
```

Description

This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device. This command is internal or hidden.

Parameter	Description
copy configured-fileserver	Copies the configured file server options like file, force-file, version, and force-version.
copy fileserver	Specify the file server details like, scp, ftp, tftp.
copy-reboot configured-fileserver	Reboots the managed devices after successful upgrade of the respective image using configured-file server options like file, force-file, version and force-version.
copy-reboot fileserver	Selects the type of supported servers like, ftp, scp, tftp and reboots the managed device post upgrade.
reboot	Reboots the managed device.

Parameter	Description
ftp	Used for mentioning FTP server.
scp	Used for mentioning SCP server.
tftp	Used for mentioning TFTP server.
file	Used for mentioning TFTP server.
force-file	Exact name of the image or image file.
force-version	Used to force the standard image name and is based on the platform type and version running on the managed device.
version	Image version and standard name based on platform type generated to load the image.

Example

The following command installs **ArubaOS_72xx_8.0.0.0-svcs-ctrl_55579** image from the configured file server on the network for a managed device with a MAC address **00:1a:1e:01:b0:b0** in partition 0:

```
(host) [mynode] #upgrade internal managed-devices copy configured-fileserver
file ArubaOS_72xx_8.0.0.0-svcs-ctrl_55579 list 00:1a:1e:01:b0:b0 partition 0
```

Command History

Release	Description
ArubaOS 8.7.0.0	This command is deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

upgrade managed-devices

upgrade managed-devices

```
ca-bundle
  update [all | path <node-path> | download url <url > | single <mac>}
  reset [all | path <node-path> | single <mac>}
copy configured-fileserver
  file <img-file> {all|path <node-path>|single <mac-addr>}
  force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
  force-my-version {all|path <node-path>|single <mac-addr>}
  force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
  my-version {all|path <node-path>|single <mac-addr>}
  version <img-version> {all|path <node-path>|single <mac-addr>}
  schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
copy fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost>
<username> <image-path>|tftp <imagehost> <image-path>}
  file <img-file> {all|path <node-path>|single <mac-addr>}
  force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
  force-my-version {all|path <node-path>|single <mac-addr>}
  force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
  my-version {all|path <node-path>|single <mac-addr>}
  version <img-version> {all|path <node-path>|single <mac-addr>}
  schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
copy-no-change-default-boot configured-fileserver
  file <img-file> {all|path <node-path>|single <mac-addr>}
  force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
  force-my-version {all|path <node-path>|single <mac-addr>}
  force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
  my-version {all|path <node-path>|single <mac-addr>}
  version <img-version> {all|path <node-path>|single <mac-addr>}
  schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
copy-no-change-default-boot fileserver {ftp <imagehost> <username> <image-
path>|scp <imagehost> <username> <image-path>|tftp <imagehost> <image-path>}
  file <img-file> {all|path <node-path>|single <mac-addr>}
  force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
  force-my-version {all|path <node-path>|single <mac-addr>}
  force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
  my-version {all|path <node-path>|single <mac-addr>}
  version <img-version> {all|path <node-path>|single <mac-addr>}
  schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
copy-reboot configured-fileserver
  file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
  force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
  partition {0|1}
  force-my-version {all|path <node-path>|single <mac-addr>}
  force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
  partition {0|1}
  my-version {all|path <node-path>|single <mac-addr>}
  version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
  schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
copy-reboot fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost>
<username> <image-path>|tftp <imagehost> <image-path>}
  file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
```

```

force-file <img-file-forced> {all|path <node-path>|single <mac-addr>}
partition {0|1}
force-my-version {all|path <node-path>|single <mac-addr>}
force-version <img-version-forced> {all|path <node-path>|single <mac-addr>}
partition {0|1}
my-version {all|path <node-path>|single <mac-addr>}
version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
schedule <year> <month> <day> <hour> <min> <sec> partition {0|1}
reboot
  all
  path <node-path>
  single <mac-addr>

```

Description

This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.



This command can only be issued on the /md node or a specific node. This command is ignored if issued on the /mynode node.

Parameter	Description
ca-bundle update	Upgrades the trusted CA certificates of managed devices.
ca-bundle reset	Resets the trusted CA certificates of managed devices.
ca-bundle download url <url>	(Optional) CA certificates will be downloaded from the specified URL. If the URL is not mentioned, the certificates will be downloaded from Activate. NOTE: The URL should begin with either http or https.
all	Upgrades/ resets the trusted CA certificates of all managed devices

Parameter	Description
path <node-path>	Upgrades/ resets the trusted CA certificates of managed devices under a specific node path. The node path must begin with /.
single <mac>	Upgrades/ resets the trusted CA certificates of a specific managed device.
copy configured-fileserver	Copies the configured file server options like file, force-file, version, and force-version.
copy fileserver	Specify the file server details like, scp, ftp, tftp.
copy-no-change-default-boot configured-fileserver	Copies upgrade image to managed devices without changing default boot using configured file server options like file, force-file, version, and force-version.
copy-no-change-default-boot fileserver	Copies upgrade image to managed devices without changing default boot using file server details like, scp, ftp, tftp.
copy-reboot configured-fileserver	Reboots the managed devices after successful upgrade of the respective image using configured-file server options like file, force-file, version and force-version.
copy-reboot fileserver	Selects the type of supported servers like, ftp, scp, tftp and reboots the managed device post upgrade
reboot	Reboots the managed device.
all	Copies/ upgrades image to all managed devices under the respective node path

Parameter	Description
path	Copies/ upgrades image under specific node path and all the managed devices under this node path target node and make them as target list.
single	Copies/ upgrades image to the specific managed device based on MAC address under the respective node-path.
ftp	Used for mentioning FTP server.
scp	Used for mentioning SCP server.
tftp	Used for mentioning TFTP server.
file	Exact name of the image or image file.
force-file	Forcing the exact image name on the file-server by ignoring the existing file or image on the managed device..
force-my-version	Used to force the master standard image name and is based on the platform type and version running on the managed device is ignored.
force-version	Used to force the standard image name and is based on the platform type and version running on the managed device.
my-version	Master Image version and standard name based on platform type generated to load the image.
version	Image version and standard name based on platform type generated to load the image.
schedule <year> <month> <day> <hour> <min> <sec>	Schedule the upgrade to occur at specified date and time.

Parameter	Description
partition	Specify the partition for the upgrade as 0 or 1.

Example

The following command schedules the upgrade of ArubaOS image on partition 0 of a single managed device with MAC address 1a:2b:3c:4d:5e:6f under the **/md** node by using an ArubaOS image from an FTP file server on the network. The upgrade is scheduled to occur at 10:30:15 AM on the 11th of December 2018.

```
(host) [md] #upgrade managed-devices copy fileserver ftp
191.1.2.3 anonymous . file ArubaOS_70xx_8.4.0.0_68198 single
1a:2b:3c:4d:5e:6f partition 0 schedule 2018 12 11 10 30 153
```

Related Commands

Command	Description
ic-cluster initiate schedule upgrade	Use this command to schedule upgrade of cluster.
show upgrade managed-devices	Use this command to view the status of scheduled upgrade of managed devices.

Command History

Release	Description
ArubaOS 8.7.0.0	The <code>ca bundle</code> parameter was introduced.
ArubaOS 8.4.0.0	The <code>schedule</code> parameter was added.
ArubaOS 8.2.0.0	The IPv6 address of the image server was added to the <code>imagehost</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

upgrade nic-firmware

upgrade nic-firmware

Description

This command upgrades the NIC firmware image.

Example

The following command reschedules the scheduled upgrade on all managed devices:

```
(host) [mynode] #upgrade nic-firmware
```

Command History

Release	Description
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

upgrade cancel-schedule

upgrade cancel-schedule

```
<year> <month> <day> <hour> <min> <sec> {all|path <node-path>|single <mac-addr>}
```

Description

This command cancels an already scheduled upgrade of the managed devices.

Parameter	Description
<year>	Specify the scheduled year in YYYY format.
<month>	Specify the scheduled month in MM format. Example: Specify 10 for October.
<day>	Specify the scheduled day of the month.
<hour>	Specify the scheduled hour in 24-hour format.
<min>	Specify the scheduled minute.
<sec>	Specify the scheduled second.
all	Cancels the scheduled upgrade on all managed devices. Target managed devices will be all managed devices under the node path.
path	Cancels the scheduled upgrade on all managed devices under the specified node path. Target managed devices will be the managed devices under the specified node path.
single <mac-addr>	Cancels the scheduled upgrade on specified managed device. Specify the MAC address of the target managed device. The managed device should be under the current node path.

Example

The following command cancels the scheduled upgrade on all managed devices:

```
(host) [mynode] #upgrade cancel-schedule 2018 12 01 23 59 59 all
```

Command History

Release	Description
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

upgrade reschedule

upgrade reschedule

```
from <from-year> <from-month> <from-day> <from-hour> <from-min> <from-sec> to  
<to-year> <to-month> <to-day> <to-hour> <to-min> <to-sec> {all|path <node-  
path>|single <mac-addr>}
```

Description

This command reschedules the existing scheduled upgrade of the managed devices.

Parameter	Description
from	Specify the original schedule.
<from-year>	Specify the originally scheduled year in YYYY format.
<from-month>	Specify the originally scheduled month in MM format. Example: Specify 10 for October.
<from-day>	Specify the originally scheduled day of the month.
<from-hour>	Specify the originally scheduled hour in 24-hour format.
<from-min>	Specify the originally scheduled minute.
<from-sec>	Specify the originally scheduled second.
to	Specify the new schedule.
<to-year>	Specify the new year in YYYY format.
<to-month>	Specify the new month in MM format. Example: Specify 10 for October.
<to-day>	Specify the new day.
<to-hour>	Specify the new hour in 24-hour format.
<to-min>	Specify the new minute.
<to-sec>	Specify the new second.
all	Reschedule the scheduled upgrade on all managed devices. Target managed devices will be all managed devices under the node path.
path	Reschedule the scheduled upgrade on all managed devices under the specified node path. Target managed devices will be the managed devices under the specified node path.

Parameter	Description
<code>single <mac-addr></code>	Reschedule the scheduled upgrade on specified managed device. Specify the MAC address of the target managed device. The managed device should be under the current node path.

Example

The following command reschedules the scheduled upgrade on all managed devices:

```
(host) [mynode] #upgrade reschedule from 2018 11 30 23 59 59 to 2018 12 25 12 30 00 all
```

Command History

Release	Description
ArubaOS 8.10.0.0	The <code>from</code> parameter is deprecated.
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

upgrade-pkg

```
upgrade-pkg
  activate <packagename>
  copy
    ftp: <ftphost> <username> <filename> flash: <destfilename>
    scp: <scphost> <username> <filename> flash: <destfilename>
    tftp: <tftphost> flash: <destfilename>
  remove
```

Description

This command upgrades the service module on Mobility Conductor.

Parameter	Description
activate <packagename>	Install and activate the service package.
copy	Download a service package through an FTP, SCP, or TFTP server.
remove	Delete a service package.

Example

This command upgrades the service module on Mobility Conductor.

```
(host) [mynode] #upgrade-pkg copy ftp: 192.0.2.22 anonymous
ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_55579 flash: ArubaOS_MM_8.0.0.0-svcs-
ctrl_appRF_55579
(host) [mynode] #upgrade-pkg activate ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_
55579
```

This command removes the service module on Mobility Conductor.

```
(host) [mynode] #upgrade-pkg remove ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_55579
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

upgrade-profile

```
upgrade-profile
  download_from_mm
  filepath
  no
  password
  protocol
  serverip
  username
  serverip
  serveraddr
```

Description

This command is used to configure the upgrade profile and can be executed only from the **/md** node-hierarchy.

Parameter	Description
download_from_mm	Download Image from MM-fileserver
filepath	File path to the location on the image server where the image file(s) reside.
no	Delete command
password	If you selected the FTP or SCP protocol for the Protocol type, enter the password that Mobility Conductor will use to connect to the image server.
protocol	Specify the protocol used to send the software upgrade from the image server to the managed device. <ul style="list-style-type: none">▪ TFTP▪ FTP▪ SCP
username <username>	If you specified FTP or SCP for the protocol parameter field, enter the user name that Mobility Conductor uses to connect to the image server.
serverip	Specify the IPv4 address of the image server. This parameter is only used by managed devices running versions prior to ArubaOS 8.2 and accepts only IPv4 address. NOTE: For FTP or SCP protocol, specify the username and password.

Parameter	Description
serveraddr	Specify the IPv4 or IPv6 address of the image server. This parameter is only used by managed devices running ArubaOS 8.2. NOTE: For FTP or SCP protocol, specify the username and password.

Example

The following command is used to upgrade managed devices:

```
(host) [md] #upgrade-profile
(host) [md] (Upgrade Profile) #serveraddr 2000:192:168:28::59
(host) [md] (Upgrade Profile) #username root
(host) [md] (Upgrade Profile) #password root123
(host) [md] (Upgrade Profile) #filepath Builds
(host) [md] (Upgrade Profile) #protocol scp
```

Command History

Release	Modification
ArubaOS 8.8.0.0	The download_from_mm parameter was added.
ArubaOS 8.2.0.0	The serveraddr parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

uplink

```
uplink
  cellular
    active
    apn <APN-Profile-Pid> <APN-name>
    backup-link
    data-limit
    frequency-band
    gps
    network-mode
    plmn
    priority
    profile
    reclassify
    speed
    uplink-id
    weight
  health-check ip {<fqdn>|<ip>}
  load-balance
    mode {hash-based|round-robin|session-count|uplink utilization}
    threshold-limits
      session-count-percent <sess_percent>
  wired
    priority <prior>
    vlan <id> uplink-id {link1|link2|link3|link4} mode hub
```

Description

Use this command to manage and configure the uplink network connection.

A managed device that supports multiple 3G cellular uplink ports in addition to their standard wired ports provides redundancy in the event of connection failure. However, at a time, only one cellular uplink is supported irrespective of many plugged-in. The **uplink health-check** configuration is required for WAN health based uplink-failover.

The uplink manager is disabled by default.

If **uplink load-balance** is enabled (active-active operation), and the device fails-over to cellular uplink because all wired uplink ports became unusable (unreachable or interface is down) then uplink load-balancing gets disabled automatically. This is because cellular uplink never participates in load-balancing of WAN traffic. Once any wired uplink port becomes usable again, cellular is disconnected and load-balancing get enabled again.

The uplink manager and load-balancing features are enabled automatically when you configure the cellular or wired uplinks.

To view the health status of an uplink on a services or managed device, issue the command [show uplink](#) in the managed device CLI. For a managed device, the health status of its uplink connections are also displayed in the **Status** section of the **Dashboard > WAN** page of the managed device WebUI.

Parameter	Description
cellular	Set the cellular uplink configuration.
active	Switch to SIM1 or SIM2 and connect to it. It will be also Boot time SIM slot select(SIM1 or SIM2).(First to connect LTE during boot or init) .
apn <APN-Profile-Pid> <APN-Name>	Specify the AP name of the cellular uplink and connection ID in modem dial string.
backup-link	Mark cellular uplink as a hot-standby uplink.
data-limit <data-limit-val>	Specify the data limit value in MB for cellular connection.
frequency-band	Specify the frequency-band configuration as 3G band or 4G band and specify Tx.Rx speed.
gps	Enable GPS.
network-mode	Specify the network mode as 3G, Auto, Custom, or LTE. By default, auto mode is set. Custom mode is not used for CLI configuration.
plmn <plmn-id>	plmn value for same carrier
priority <prior>	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary link. 1-255
profile	Cellular interface profile.
reclassify	Re-init cellular uplink connection - Reboot not needed.
speed <cellular_speed>	Configure maximum cellular uplink speed in Mbps. 1-1000

Parameter	Description
uplink-id <name>	Identifier(name) for cellular uplink.
weight <cellular_weight>	Weight of this cellular uplink (used in load-balancing) 1-100
load-balance	Load-balance configuration.
mode hash-based round-robin session-count uplink-utilization	Choose one of the following load balancing modes: <ul style="list-style-type: none"> ▪ Hash based: Hash-based load balancing uses information from the packets being sent, (e.g. the source IP address, destination IP address, protocol and port numbers to determine how to load balance that traffic) ▪ Round Robin: Traffic is equally distributed to all the active uplinks ▪ Session Count: Traffic is balanced between the uplink ports based on the number of sessions managed by each link. The session-distribution is guided by uplink load-balance threshold-limits session-count <> percentage. ▪ uplink-utilization: Use available uplink capacity to load-balance.
threshold-limits	Define threshold limits for load balancing.
session-count-percent <sess_perc>	Specify the maximum percentage of total sessions that can be managed by any active uplink. The default % is equally distributed among the number of wired uplink ports present. That is: <ul style="list-style-type: none"> ▪ For 4 uplink ports- 25% ▪ For 3 uplink ports- 33% ▪ For 2 uplink ports- 50% ▪ For 1 uplink port- 100%

Parameter	Description
threshold-limits	Set threshold limits for load balancing. The valid value is session count percentage.
health-check {ip {<fqdn> <ip>}}	The <code>health-check</code> parameter is introduced to monitor the availability and quality of the connection to a master/conductor managed device with the specified FQDN or IP address.
wired	Define the wired uplink configuration.
priority <prior>	Define the default priority for wired uplinks. 1-255 200.
vlan <id> uplink-id {link1 link2 link3 link4}	Define the VLAN ID of the uplink VLAN. A maximum of four wired VLANs can be defined. 1-4094
mode	Specify the operating mode of the uplink.
hub	Specify that this uplink accepts overlay connection from spoke devices.

Related Commands

Command	Description
show uplink	Displays uplink configuration details.

Command History

Release	Modification
ArubaOS 8.4.0.0	The following sub-parameters were deprecated: <ul style="list-style-type: none"> ■ <code>enable</code> ■ <code>media-mode</code>

Release	Modification
	<ul style="list-style-type: none"> ▪ jitter <avg_jitter> ▪ latency <avg_latency> ▪ priority <wired_vlan_priority>
ArubaOS 8.1.0.0	The load-balance and wired parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

usb

usb

```
reclassify <address> [<bus>]  
re-configure internal-modem
```

Description

This command disconnects and reclassifies a USB device connected to a managed device.

Parameter	Description
reclassify <address>	Disconnect and reclassify a USB device.
re-configure internal-modem	Reconfigure the internal LTE modem.

Example

This command disconnects and reclassifies a USB device with an address of 18 connected to a managed device.

```
(host-md) #usb reclassify 18
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

user-role

```
user-role <name>
  access-list {eth|mac|session} <acl> [ap-group <group>] [position <number>]
  bw-contract
    app <appname> <bw-contract_name> {downstream|upstream}
    appcategory <appcategory-name> <bw-contract_name> {downstream|upstream}
    exclude {app|appcategory}
    web-cc-category <web-cc-category-name> <bw-contract_name>
      {downstream|upstream}
    web-cc-reputation {high-risk|low-risk|moderate-risk|suspicious|trustworthy}
      <bw-contract_name> {downstream|upstream}
      <bw-contract-name> [per-user|per-apgroup] {downstream|upstream}
  captive-portal {<STRING>|check-for-accounting}
  dialer <name>
  dpi
  ip-classification
  max-sessions <number>
  no ...
  openflow-enable
  pool {l2tp|pptp|via-dhcp} <name>
  qos-profile <profile>
  reauthentication-interval [<minutes>|<seconds>]
  registration-role
  robust-age-out
  sso <profile>
  stateful-kerberos <profile>
  stateful-ntlm <ntlm_profile_name>
  via <profile>
  vlan {VLAN ID|VLAN name}
  web-cc disable
  wispr <wispr_profile_name>
```

Description

This command configures a user role.

Every client in a user-centric network is associated with a user role. All wireless clients start in an initial role. From the initial role, clients can be placed into other user roles as they pass authentication.

Parameter	Description
<name>	Role name
access-list	Type of ACL to be applied: eth: Ethertype ACL, configured with the <code>ip access-list eth</code> command.

Parameter	Description
	<p>mac: MAC ACL, configured with the <code>ip access-list mac</code> command.</p> <p>session: Session ACL, configured with the <code>ip access-list session</code> command.</p>
<acl>	Name of the configured ACL.
ap-group	(Optional) AP group to which this ACL applies.
position	<p>(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.</p> <p>Default: (last)</p>
bandwidth-contract	Name of a bandwidth contract or rate limiting policy configured with the <code>aaa bandwidth-contract</code> command. The bandwidth contract must be applied to either downstream or upstream traffic.
app	<p>Name of the application bandwidth contract configured for the user role. The bandwidth contract must be applied to either downstream or upstream traffic.</p> <p>NOTE: For a complete list of supported applications, issue the command <code>show dpi application all</code>.</p>
appcategory	<p>Name of the application category bandwidth contract configured for the user role. The bandwidth contract must be applied to either downstream or upstream traffic.</p> <p>NOTE: For a complete list of supported applications, issue the command <code>show dpi application category all</code>.</p>
web-cc-category web-cc-reputation <cc-name> <bwc-name>	<p>Apply a bandwidth contract to the specified web content category or reputation level. Bandwidth contracts can be applied to user-defined web content categories created using the <code>web-cc</code> command. The five web content reputation levels are predefined in ArubaOS.</p> <p>NOTE: bandwidth contracts applied to a web content category or reputation will not be enforced</p>

Parameter	Description
	<p>unless web content classification is enabled using the <code>firewall web-content-classification</code> command.</p> <p>Range: Available reputation categories are:</p> <ul style="list-style-type: none"> ■ high-risk ■ low-risk ■ moderate-risk ■ suspicious ■ trustworthy
<code>exclude app appcategory</code>	<p>Excludes an application or application category from being configured as a bandwidth contract.</p>
<code>downstream</code>	<p>Applies the bandwidth contract to traffic from the controller to the client.</p>
<code>per-user</code>	<p>Specifies that bandwidth contract is assigned on a per-user basis instead of a per-role basis. For example, if two users are active on the network and both are part of the same role with a 500 Kbps bandwidth contract, then each user is able to use up to 500 Kbps.</p> <p>Default: (per role)</p>
<code>upstream</code>	<p>Applies the bandwidth contract to traffic from the client to the controller.</p>
<code>captive-portal <STRING></code>	<p>Name of the captive portal profile configured with the <code>aaa authentication captive-portal</code> command.</p>
<code>check-for-accounting</code>	<p>If disabled, RADIUS accounting is done for an authenticated users irrespective of the captive-portal profile in the role of an authenticated user. If enabled, accounting is not done as long as the user's role has a captive portal profile on it. Accounting will start when Auth/XML-Add/CoA changes the role of an authenticated user to a role which doesn't have captive portal profile.</p> <p>Default: Enabled</p>
<code>dialer</code>	<p>If VPN is used as an access method, name of the VPN dialer configured with the <code>vpn-dialer</code> command. The user can login using captive portal and download the dialer. The dialer is a Windows application that configures the VPN client.</p>
<code>dpi</code>	<p>Role specific DPI configuration.</p>

Parameter	Description
disable	Disable role specific DPI configuration.
ip-classification	Role specific ip-classification configuration.
disable	Disable role specific ip-classification configuration.
max-sessions	Maximum number of datapath sessions per user in this role. Range: 0-65535 Default: 65535
no	Negates any configured parameter.
openflow-enable	Enables SDN for the user role. Default: Enabled
pool	If VPN is used as an access method, specifies the IP address pool from which the user's IP address is assigned: <ul style="list-style-type: none"> ■ l2tp: When a user negotiates an L2TP or IPsec session, specifies an address pool configured with the <code>ip local pool</code> command. ■ pptp: When a user negotiates a PPTP session, specifies an address pool configured with the <code>pptp ip local pool</code> command. ■ via-dhcp: Defines an external DHCP server address instead of internal L2TP pool and the managed device gets the IP address from an external DHCP server. <p>NOTE: L2TP pool and DHCP pool configuration in a role are mutually exclusive.</p>
<name>	Name of the L2TP or PPTP or DHCP pool to be applied.
qos-profile	Applies a QOS profile to the user role.
reauthentication-interval	Interval, in minutes or seconds, after which the client is required to reauthenticate. Range: 0-4096 in minutes <ul style="list-style-type: none"> ■ 0-245760 in seconds Default: 0(disabled)
registration-role	If enabled, a user is forced to do MAC-based authentication every time the user connects to the network. Default: disabled
robust-age-out	Apply Robust Age-out mechanism on wired passive clients.

Parameter	Description
	<p>Default: Disabled.</p> <p>NOTE: This feature impacts system load and performance. Enable this mechanism for a limited number of clients only.</p>
sso	Applies an SSO profile to the user role.
stateful-kerberos	Applies a stateful Kerberos profile to the user role.
stateful-ntlm	Apply stateful NTLM authentication to the specified user role
via	Applies a VIA connection profile to the user role.
vlan	<p>Identifies the VLAN ID or VLAN name to which the user role is mapped. This parameters works only when using Layer-2 authentication such as 802.1X or MAC address, ESSID, or encryption type role mapping because these authentications occur before an IP address is assigned. If a user authenticates using a Layer-3 mechanism such as VPN or captive portal this parameter has no effect.</p> <p>NOTE: VLAN IDs and VLAN names cannot be listed together.</p>
voip-profile	Applies a VOIP profile to the user role.
web-cc disable	<p>Disable web content classification for this user role. User role bandwidth contracts associated with web content classification categories and reputation types will not enforced unless web content classification is enabled using the <code>firewall web-content-classification</code> command.</p>
wispr	Apply WISPr authentication to the specified user role.

Example

The following command configures a user role:

```
(host)[md](config) #user-role new-user
dialer default-dialer
pool pptp-pool-1
```

Command History

Release	Modification
ArubaOS 8.8.0.0	Added a new sub-parameter, <code>via-dhcp</code> , to support external DHCP server address pool instead of internal L2TP pool. Added a new parameter, <code>robust-age-out</code> , to apply a new age-out mechanism on wired passive clients.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Conductor.

valid-network-oui-profile

```
valid-network-oui-profile
no
oui <oui>
```

Description

This command allows you to add a new OUI to the managed device. The new OUI must be entered in a aa:bb:cc format.

Parameter	Description
no	Negates any configured parameter.
oui <oui>	The new OUI to be added. Use the aa:bb:cc format to input the new OUI.

Example

The following example adds a new OUI to the managed device.

```
(host) [mynode] (config) #valid-network-oui-profile
(host) [mynode] (Valid Equipment OUI profile) #
(host) [mynode] (Valid Equipment OUI profile) #oui 00:11:22
This should only be used when adding equipment with a new OUI. Are you sure
you
want to proceed? [y/n]: y
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

vlan-bwcontract-explist

```
vlan-bwcontract-explist mac <mac>
```

Description

This command adds entries to or remove entries from the MAC exception list for bandwidth contracts on broadcast or multicast traffic. Bandwidth contracts on a VLAN can limit broadcast and multicast traffic. ArubaOS includes an internal exception list to allow broadcast and multicast traffic using the VRRP, LACP, OSPF, PVST and STP protocols. To remove per-vlan bandwidth contract limits on an additional broadcast or multicast protocol, add the MAC address for that broadcast or multicast protocol to the Vlan Bandwidth Contracts MAC Exception List.

Parameter	Description
<mac>	MAC address of a protocol that should be added to or removed from the exception list for bandwidth contracts.

Example

The following example adds the MAC address for CDP and VTP to the list of protocols that are not limited by VLAN bandwidth contracts.

```
(host) [mynode] (config) #vlan-bwcontract-explist mac 01:00:0C:CC:CC:CC
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vlan-name

```
vlan-name <name> [assignment even {ip-timeout | max-ip-timeouts | full-period} | hash]
```

Description

This command creates a named VLAN on the managed device and given an assignment type.

Parameter	Description
<name>	Name of the VLAN.
assignment	Sets the assignment type as one of the following : <ul style="list-style-type: none">▪ even: This is based on an even distribution of VLAN pool assignments.▪ hash: This is based on the station MAC address.
auto-disconnect	Enables VLAN Resiliency. Client auto disconnection on IP timeout 0-180 3
ip-timeout	Enables VLAN pooling resiliency. Configures the timeout value, in seconds, before declaring a client's DHCP request as timed out. 0-180 3
max-ip-timeouts	Configures the maximum number of IP timeouts allowed before marking the VLAN as full. 1-128 3
full-period	Time period, in seconds, for a VLAN to be marked as full. 30-3600 30

Create a named VLAN so you can set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-managed device networks from a single location.



VLAN pooling should *not* be used with static IP addresses.



Perform **vlan-name** configuration changes with caution. All **vlan-name** configuration changes requires reconfiguration of all the VAPs. For large VLAN deployments it is recommended to perform **vlan-name** configuration changes during a planned maintenance window.

The Even VLAN assignment type maintains a dynamic latest usage level of each VLAN ID. Therefore, as users age out, the number of available addresses increases. This leads to a more even distribution of addresses.

The Even type is only supported in tunnel and decrypt tunnel forwarding modes. It is not supported in split or bridge modes and it is not allowed for VLAN pools that are configured directly under a virtual AP. It can only be used under named VLANs. If a VLAN is given an Even assignment in bridge mode, a message displays indicating that the Hash assignment is automatically used instead to retrieve the VLAN ID.



L2 Mobility is not compatible with the existing implementation of the Even VLAN pool assignment type.

Example

The following example creates a VLAN named **mygroup** with the assignment type “even” on the managed device:

```
(host) [mynode] (config) #vlan-name mygroup assignment even
```

Related Commands

Command	Description
show vlan status	Shows the VLAN status.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>ip-timeout</code> , <code>max-ip-timeouts</code> and <code>full-period</code> sub-parameters were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vlan

```
vlan [<id> option-82] | [<name> <vlan-ids>] | [range remove <WORD> ] | [wired aaa-profile <profile>]
```

Description

This command creates a VLAN ID or a range of VLAN IDs on the managed device. Use the `vlan-name` command to create a named VLAN to set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-managed device networks from a single location.

To enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device, you must use the `wired aaa-profile` parameter to specify the wired AAA profile you would like to apply to that VLAN. If you do not specify a per-VLAN wired AAA profile, traffic from clients connected to an untrusted wired port or VLAN will use the global wired AAA profile, if configured.

Parameter	Description
<id>	Identification number for the VLAN. 2-4094 1
option-82	Turn on Option-82
<name>	(Optional) Identification name of the VLAN. The VLAN name was created using the <code>vlan-name</code> command. 1-32 characters; a name cannot begin with a numeric character VLAN<id>
<vlan-ids>	(Optional) List of VLAN IDs that are associated with this VLAN. If two or more IDs are listed, the VLAN needs to be specified first as a VLAN pool using the <code>vlan-name</code> command. Existing VLAN IDs 1
range <range>	Create a range of multiple VLAN IDs by specifying the beginning and ending VLAN ID separated by a hyphen. For example, 55-58 2-4094
remove <WORD>	List a range of vlans to be removed and it is a comma and a '-' separated list of vlans.

Parameter	Description
wired aaa-profile <profile>	Assign an AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device. This parameter applies to wired clients only. Note that this profile will only take effect if the VLAN or the port on the managed device is untrusted. If both the port and the VLAN are trusted, no AAA profile is assigned.

Example

The following example creates VLAN ID 27 with the description **myvlan** on the managed device.

```
(host) [mynode] (config) #vlan 27 myvlan
```

The following example associates the VLAN IDs 5, 12 and 100 with VLAN guestvlan on the managed device.

```
vlan guestvlan 5,12,100
```

The following example creates VLAN IDs 200-300, 302, 303-400.

```
(host) [mynode] (config) #vlan range 200-300,302, 303-400
```

Related Commands

Command	Description
show vlan	This command shows a configured VLAN interface number, description and associated ports
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vpn-acl

```
vpn-acl route <vpnraclname> | session <vpnsaclname>
```

Description

This command configures both session and route ACL for branch-vpnc tunnel.

Parameter	Description
route <vpnraclname>	This parameter configures route ACL on branch-vpnc tunnel traffic
session <vpnsaclname>	This parameter configures session ACL on branch-vpnc tunnel traffic.

Example

The following example configures route ACL on branch-vpnc tunnel:

```
(host) [mynode] (config) #vpn-acl route test
```

Command History

Release	Modification
ArubaOS 8.6.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base Operating System	Config mode on Mobility Conductor.

vpn-dialer

```
vpn-dialer <name>
  enable dnetclear|l2tp|pptp|securid_newpinmode|wirednowifi
  ike {authentication {pre-share <key>|rsa-sig}|encryption {3des|des}}|
  group {1|2}|hash {md5|sha}|lifetime [<seconds>]}
  ipsec {encryption {esp-3des|esp-des}|hash {esp-md5-hmac|esp-sha-hmac}}|
  lifetime [<seconds>]|pfs {group1|group2}}
  no {enable...|ipsec...|ppp...}
  ppp authentication {cache-securid|chap|mschap|mschapv2|pap}
```

Description

This command configures the VPN dialer. A VPN dialer is a Windows application that configures a Windows client for use with the VPN services in the managed device. When VPN is used as an access method, a user can login using captive portal and download a VPN dialer. You can customize a VPN dialer for a user role configured with the `user-role` command. After the user authenticates via captive portal, a link appears to allow download of the VPN dialer if a dialer is configured for the user role.

Parameter	Description
<name>	Name that identifies this VPN dialer configuration.
enable	Enables dialer operations:
dnetclear	Enables “split tunneling” functionality so that traffic destined for the internal network is tunneled while traffic for the Internet is not. This option is not recommended for security reasons. Default: disabled
l2tp	Allows the dialer to negotiate a Layer-2 Tunneling Protocol (L2TP)/IPsec tunnel with the managed device. Default: enabled
pptp	Allows the dialer to negotiate a Point-to-Point Tunneling Protocol (PPTP) with the managed device. Default: disabled
securid_newpinmode	Supports SecurID new and next pin mode. Default: disabled
wirednowifi	Allows the dialer to detect when a wired network connection is in use, and shuts down the wireless interface. Default: disabled

Parameter	Description
ike	Configures internet key exchange (IKE) protocol. This configuration must match the IKE policy configured with the <code>crypto isakmp policy</code> command on the managed device.
authentication	Specifies whether preshared keys or RSA signatures are used for IKE authentication. Range: pre-share rsa-sig Default: pre-share
encryption	Specifies the IKE encryption protocol, either DES or 3DES. Range: 3des des Default: 3des
group	Specifies the Diffie-Hellman group, either 1 or 2. Range: 1 2 Default: 2
hash	Specifies the HASH algorithm, ether SHA or MD5. Range: md5 sha Default: sha
lifetime	Specifies how long an IKE security association lasts, in seconds. Range: 300-86400 Default: 28800 seconds
ipsec	Configures IPsec. This configuration must match the IPsec parameters configured with the <code>crypto dynamic-map</code> and <code>crypto ipsec</code> commands on the managed device.
encryption	Specifies the encryption type for IPsec, either DES or 3DES. Range: esp-3des esp-des Default: esp-3des
hash	Specifies the hash algorithm used by IPsec, either MD5 or SHA. Range: esp-md5-hmac esp-sha-hmac Default: esp-sha-hmac
lifetime	Specifies how long an IPsec security association lasts, in seconds. Range: 300-86400 Default: 7200 seconds
pfs	Specifies the IPsec Perfect Forward Secrecy (PFS) mode, either group 1 or group 2. Range: group1 group2 Default: group2

Parameter	Description
no	Negates any configured parameter.
ppp authentication	Enables the protocols for PPP authentication. This list should match the L2TP or PPTP configuration configured with the <code>vpdn</code> command on the managed device.
cache-securid	The managed device caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost. Default: disabled
chap	Use CHAP with PPP authentication. Default: enabled
mschap	Use MSCHAP with PPP authentication. Default: enabled
mschapv2	Use MSCHAPv2 with PPP authentication. Default: enabled
pap	Use PAP with PPP authentication. Default: enabled

Example

The following example configures a VPN dialer:

```
(host) [node] (config) #vpn-dialer default-dialer
ike authentication pre-share f00xYz123BCA
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

vpdn group l2tp

```
vpdn group l2tp
  client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
  disable|enable
  l2tp tunnel hello <seconds>
  no ...
  ppp authentication {CACHE-SECURID|CHAP|EAP|MSCHAP|MSCHAPv2|PAP}
  ppp securid cache <minutes>
```

Description

This command configures an L2TP or IPsec VPN connection. L2TP or IPsec relies on the PPP connection process to perform user authentication and protocol configuration. You must specify the protocol used for PPP authentication and whether SecureID tokens are cached on the managed device. Client addresses are assigned from a pool configured with the `ip local pool` command.

Parameter	Description
<code>client configuration</code>	Configures parameters for the remote clients.
<code>dns</code>	Configures a primary and optional secondary DNS server.
<code>wins</code>	Configures a primary and optional secondary WINS server.
<code>disable enable</code>	Disables or enables termination of L2TP clients. Default: Enabled
<code>l2tp tunnel hello</code>	Configures L2TP tunneling hello timeout, in seconds. Range: 10-1440 Default: 60 seconds
<code>no</code>	Negates any configured parameter.
<code>ppp authentication</code>	Enables the protocols for PPP authentication. This list should match the L2TP configuration configured with the <code>vpn-dialer</code> command on the managed device.
<code>CACHE-SECURID</code>	The managed device caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.
<code>CHAP</code>	Use CHAP with PPP authentication.

Parameter	Description
EAP	Use EAP-TLS with PPP authentication. Specify this protocol for Windows IPsec VPN clients that use Common Access Card (CAC) Smart Cards that contain user information and digital certificates.
MSCHAP	Use MSCHAP with PPP authentication.
MSCHAPv2	Use MSCHAPv2 with PPP authentication. This is the default for L2TP
PAP	
ppp securid	If CACHE-SECURID is configured for PPP authentication, this specifies the time, in minutes, that the token is cached. Range: 15-10080 Default: 1440 minutes

Example

The following example configures virtual private dial-in networking:

```
(host) [mynode] (coinfig) #vpdn group l2tp
ppp authentication PAP
client configuration dns 10.1.1.2
client configuration wins 10.1.1.2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vpdn group pptp

```
vpdn group pptp
  client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
  disable|enable
  no ...
  ppp authentication {MSCHAP|MSCHAPv2}
  pptp echo <seconds>
```

Description

This command configures a PPTP VPN connection. PPTP connections require user-level authentication through a PPP authentication protocol (MSHCAV2 is the currently-supported method.) Client addresses are assigned from a pool configured with the `ppp` command.

Parameter	Description
<code>client configuration</code>	Configures parameters for the remote clients.
<code>dns</code>	Configures a primary and optional secondary DNS server.
<code>wins</code>	Configures a primary and optional secondary WINS server.
<code>disable enable</code>	Disables or enables termination of PPTP clients. Default: Enabled.
<code>no</code>	Negates any configured parameter.
<code>ppp authentication</code>	Enables the protocols for PPP authentication. This list should match the PPTP configuration configured with the <code>vpdn-dialer</code> command on the managed device.
<code>MSCHAP</code>	Use MSCHAP with PPP authentication.
<code>MSCHAPv2</code>	Use MSCHAPv2 with PPP authentication. This is the default for L2TP
<code>pptp echo</code>	Time, in seconds, that the managed device waits for a PPTP echo response from the client before considering the client to be down. The client is disconnected if it does not respond within this interval. Range: 10-300 Default: 60 seconds.

Example

The following example configures virtual private dial-in networking:

```
vpdn group pptp
ppp authentication MSCHAPv2
client configuration dns 10.1.1.2
client configuration wins 10.1.1.2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vpnip

```
vpnip <vpncip>|v6 <vpncipv6>
  ipsec-custom-cert vpnc-mac-1-c <mac-addr> [vpnc-mac-2-c <mac-addr>] [ca-cert
  <ca>|factory-ca-cert] [fqdn <local-fqdn>] [interface vlan <id>] [server-cert
  <sc>|factory-cert] [suite-b gcm128 |gcm256]
  ipsec-factory-cert vpnc-mac-1 <mac-addr>
  peer-mac <peer-mac-1> ipsec <key> {[fqdn <local-fqdn>] [interface vlan
  <vpnvlanid>]}
```

Description

This command configures the certificate or PSK used by a managed device to create a site-to-site IPsec VPN tunnel to a controller configured as a VPN concentrator. Use this command to configure a managed device to communicate with a VPN concentrator in a deployment where both Mobility Conductor and the VPN concentrator are located within the same DMZ.

When the managed device communicates with the VPN concentrator to set up an IPsec tunnel, any uplink VLAN tag defined via the [uplink wired](#) command will be sent with the vendor-id during IKE negotiation. This setting can uniquely bind the tunnel from a particular uplink on a managed device to a corresponding crypto map on VPN concentrator.

Parameter	Description
<vpncip>	Configure the IPv4 address of the VPN concentrator.
v6 <vpncipv6>	Configure the IPv6 address of the VPN concentrator.
ipsec-custom-cert	Custom Cert-based IPsec secure communication between a VPN concentrator and a managed device.
vpnc-mac-1-c <mac-addr>	Specify the first VPN concentrator's MAC address.
vpnc-mac-2-c <mac-addr>	Specify the second VPN concentrator's MAC address.
ca-cert <ca> factory-cert	The specified CA certificate will be used to validate the certificate presented by the VPN concentrator. Enter a name of a CA certificate, or choose factory-cert to use factory-installed CA Cert chain.
fqdn <local-fqdn>	The managed device's FQDN (max 64 bytes) used in IKE. This is optional for a dynamically addressed device.
interface vlan <id>	Specify the VLAN ID of a VLAN interface that initiates the IKE tunnel. If no interface is specified, the managed device uses the switch IP.
server-cert <sc> factory-cert]	The managed device will use the specified server certificate for IPsec communication to a VPN concentrator.

Parameter	Description
<code>suite-b gcm128 gcm256</code>	Specify the GCM-128 or GCM-256 Suite B Algorithm
<code>ipsec-factory-cert</code>	Factory Cert-based IPsec secure communication between the VPN concentrator and the managed device.
<code>vpnc-mac-1-c <mac-addr></code>	Specify VPN concentrator's MAC address.
<code>peer-mac <peer-mac-1></code>	Specify Peer MAC address for PSK-based authentication.
<code>ipsec <key></code>	Enable IPsec secure communication between the VPN concentrator and the managed device using the specified key.
<code>fqdn <local-fqdn></code>	The managed device's FQDN (max 64 bytes) used in IKE. This is optional for a dynamically addressed device.
<code>interface vlan <vpnvlanid></code>	Specify the VLAN ID of a VLAN interface that initiates the IKE tunnel. If no interface is specified, the managed device uses the switch IP.

Example

The following example configures a factory certificate used by a managed device to create a site-to-site IPsec VPN tunnel to a controller configured as a VPN concentrator:

```
[host] (mynode) (config) # vpnip 192.0.0.2 ipsec-factory-cert vpn-mac-1
01:00:5E:00:00:01
```

Related Commands

Command	Description
uplink	Manage and configure the uplink network connection on a managed device.
vpnip	Defines Internet Key Exchange (IKE) parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device.

Command History

Release	Modification
ArubaOS 8.7.0.0	The <code>v6 <vpncipv6></code> parameter was added.
ArubaOS 8.2.0.0	The <code>vpnc-mac-2-c</code> sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

vpn-peer peer-mac

```
vpn-peer peer-mac <mac-addr>  
  cert-auth {ca-cert <peer-ca> server-cert <peer-sc>}|factory-cert} suite-B  
  {gsm128|gsm256}  
  pre-share-key <peer-key> suite-B {gsm128|gsm256}
```

Description

This command defines IKE parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device. Use this command on controller configured as a VPN concentrator to define a VPN between that device and another managed device. When the other managed device communicates with the VPN concentrator to set up an IPsec tunnel, any uplink VLAN tag defined via the [uplink wired](#) command will be sent with the vendor-id during IKE negotiation. This setting can uniquely bind the tunnel from a particular uplink on a managed device to a corresponding crypto map on VPN concentrator.

Parameter	Description
peer-mac <mac-addr>	MAC address of the managed device. If the peer device is an x86 server, then configure the MAC address of the management interface of the managed device. However, if the peer device is a hardware platform, you must provide the MAC address of the VLAN interface of the managed device.
cert-auth	Enable certificate authentication.
ca-cert <peer-ca>	<peer-ca> is a user-defined name of a trusted CA certificate installed on the VPN concentrator. This CA certificate will be used validate the certificate presented by the managed device.
server-cert <peer-sc>	<peer-SC> is a user-defined name of a server certificate installed on the VPN concentrator. The VPN concentrator will use the specified server certificate for IPsec communication to a managed device.
factory-cert	The factory-installed CA certificate on the VPN concentrator will be used validate the certificate presented by the managed device.
suite-b {gsm128 gsm256}	Specify one of the following Suite B Algorithm: <ul style="list-style-type: none">■ gcm128: Suite B AES-GCM Algorithm parameter (128 bits)■ gcm256: Suite B AES-GCM Algorithm parameter (256 bits)
pre-share-key <peer-key>	Enable authentication using a PSK.

Parameter	Description
<code>suite-b {gsm128 gsm256}</code>	Specify one of the following Suite B Algorithm: <ul style="list-style-type: none"> ■ gcm128: Suite B AES-GCM Algorithm parameter (128 bits) ■ gcm256: Suite B AES-GCM Algorithm parameter (256 bits)

Example

The following example configures a VPN from a managed device VPN concentrator to another managed device using the factory default certificate:

```
(host)[node] (config) #vpn-peer peer-mac 01:00:5E:00:00:FF factory-cert
```

Related Commands

Command	Description
vpnip	Configures the certificate or PSK used by a managed device to create a site-to-site IPsec VPN tunnel to a VPN concentrator.
vpn-peer peer-mac	Defines IKE parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device.
uplink	Manages and configure the uplink network connection on a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Conductor.

vpn-peer pass-code

```
vpn-peer pass-code <auth-pass-code>  
  cert-auth {ca-cert <peer-ca> server-cert <peer-sc>}|{factory-cert}
```

Description

This command automates the process of whitelisting/allowlisting the branch devices to avoid extra configuration for each device at the headend. For automatic whitelisting/allowlisting of managed devices in the VPN Concentrator, the authentication code method is used. In this method, the whitelisting/allowlisting of the device is achieved through the authentication token. You must configure the same VPN peer authentication passcode on the Mobility Conductor as well as the VPN Concentrator to whitelist/allowlist the device in the database.

Parameter	Description
pass-code <auth-pass-code>	The authenticate token to be configured on Mobility Conductor as well as the VPN Concentrator. The Mobility Conductor pushes this configuration to the managed devices for automatic whitelisting/allowlisting on the VPN Concentrator.
cert-auth	Enable certificate authentication.
ca-cert <peer-ca>	<peer-ca> is a user-defined name of a trusted CA certificate installed on the VPN concentrator. This CA certificate is used to validate the certificate presented by the managed device.
server-cert <peer-sc>	<peer-SC> is a user-defined name of a server certificate installed on the VPN concentrator. The VPN concentrator uses the specified server certificate for IPsec communication to a managed device.
factory-cert	The factory-installed CA certificate on the VPN concentrator will be used validate the certificate presented by the managed device.

Example

The following example configures an authentication code on the Mobility Conductor, which is used for automatic whitelisting/allowlisting of managed devices on a VPN concentrator where the same authenticate code is configured.

```
(host)[mynode] (config) #vpn-peer pass-code Arubal23 cert-auth factory-cert
```

Command History

Release	Modification
ArubaOS 8.9.0.0	All instances of <code>whitelist</code> have been replaced with <code>allowlist</code> .
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

vrrp

```
ipv6 <id>  
  advertise <interval>  
  authentication <password>  
  description <text>  
  holdtime <secs>  
  ipv6  
  no...  
  preempt  
  priority <level>  
  shutdown  
  tracking {interface|master-up-time|vlan|vrrp-master-state}  
  vlan <vlanid>
```

Description

This command configures the VRRP. Use this command to set parameters for VRRP on the Mobility Conductor. The default VRRP parameters can be left for most implementations.

You can use a combination of numbers, letters, and characters to create the authentication password and the VRRP description. To include a space in the password or description, enter quotation marks around the string. For example, to create the password Floor 1, enter "Floor 1" at the prompt.

To change the existing password or description, enter the command with a different string. The new password or description takes affect immediately.

To unconfigure the existing password or description, enter "" at the prompt. If you update the password on one managed device, you must update the password on the redundant member pair.

Parameter	Description
id	<p>Number that uniquely identifies the VRRP instance, also known as the VRID. This number should match the VRID on the other member of the redundant pair.</p> <p>For ease in administration, you should configure this with the same value as the VLAN ID.</p> <p>After you configure the VRID, the command platform enters VRRP mode. From here, you can access the remaining VRRP commands.</p> <p>1-255</p>

Parameter	Description
ipv6	Include this optional parameter to define a VRRP using an IPv6 address.
advertise	<p>Specifies the time, in seconds, between successive VRRP advertisements sent by the current <i>master</i>. Best practices are to use the default value.</p> <p>1-60 seconds 1 second</p>
authentication	<p>Configure an optional password of up to eight characters to be used to authenticate VRRP peers in their advertisements. The password must be the same on both members of the redundant pair. The password is sent in plain-text and therefore should not be treated as a security measure. Rather, the purpose of the password is to guard against misconfigurations in the event that other VRRP devices exist on the same network. This parameter is supported only for IPv4.</p> <p>8 characters</p>
description	<p>Configure an optional text string to describe the VRRP instance.</p> <p>1-80 characters</p>
holdtime <secs>	<p>The VRRP virtual router does not begin listening to advertisements until the holdtime expires. If your deployment includes a VRRP master with preemption disabled and an uplink switch is running RSTP, a higher value will prevent the VRRP master from regaining the master state after it reboots. The holdtime is disabled by default. If enabled without mentioning a time range, the holdtime will be configured to the default value, 45 seconds.</p> <p>30-120 seconds Disabled</p>

Parameter	Description
<code>ipv6 address</code>	<p>Configure the virtual IPv6 address that will be owned by the elected VRRP <i>master</i>. Use the same IPv6 address on each member of the redundant pair.</p> <p>This IPv6 address will be redundant - it will be active on the VRRP master, and will become active on the VRRP backup in the event that the VRRP master fails.</p> <p>The IPv6 address must be unique; the IPv6 address cannot be the loopback address of the Mobility Conductor. Only IPv6 address formats are supported. Starting from ArubaOS 8.2.1.0, you can configure a unique local address as the VRRP IPv6 address on the Mobility Conductor and the managed devices.</p>
<code>no</code>	<p>Negates all configured VRRP parameters.</p>
<code>preempt</code>	<p>Preempt mode allows a managed device to take over the role of master if it detects a lower priority managed device currently acting as master.</p> <p>Best practices are to use the default value to avoid excessive interruption to users or “flapping” if a problematic managed device is cycling up and down.</p> <p>Disabled</p>
<code>delay</code>	<p>Delay value in seconds.</p> <p>Specifying a value enables the delay timer. The timer is triggered when the VRRP state moves out of backup or init state to become a master. This is applicable only if router pre-emption is enabled.</p> <p>When the timer is triggered, it delays the router for a specified period of time before taking over the master router. In the mean time, if there is an advertisement from another VRRP master (existing master), the router stops the timer and does not transition to master.</p> <p>0-60 seconds</p>

Parameter	Description
	0
<pre>priority</pre>	<p>Defines the priority level of the VRRP instance for the Mobility Conductor. This value is used in the election mechanism for the master. A higher number specifies a higher priority.</p> <p>The default priority setting is adequate for most networks.</p> <p>1-255</p> <p>100</p>
<pre>shutdown</pre>	<p>Administratively shutdown VRRP. When down, VRRP is not active, although the Mobility Conductor maintains the configuration information.</p> <p>To start the VRRP instance, use no shutdown.</p> <p>Enabled</p>
<pre>tracking</pre>	<p>Alter the virtual router priority value.</p>
<pre>interface {gigabitethernet <slot/module/port>} {sub <value>}</pre>	<p>Configures VRRP tracking based on Layer-2 interface state transitions. You can track a combined maximum of 16 VLAN and Layer-2 interfaces.</p> <ul style="list-style-type: none"> ■ <slot/module/port> - Interface in <slot>/<module>/<port> format. ■ sub - Decreases the priority of the VRRP instance by the specified number. When the interface comes up again, the value is restored to the previous priority level. The combined priority and tracking vales cannot exceed 255. If the priority value exceeds 255, the Mobility Conductor displays an error message. Valid range is 0-255.
<pre>master-up-time <duration> add <value></pre>	<p>The VLAN tracking feature monitors how long the Mobility Conductor has been master for the VRRP instance.</p> <ul style="list-style-type: none"> ■ duration - This value configures the number of

Parameter	Description
	<p>minutes that must elapse before uptime tracking takes place. Valid range is 0-1440 minutes.</p> <ul style="list-style-type: none"> ■ add - Instructs the Mobility Conductor to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. Valid range is 0-255. If the priority value exceeds 255, the Mobility Conductor displays an error message similar to the following - Error: Vrrp 30 priority + tracking value exceeds 255.
<pre>vlan <vlanid> {sub <value>}</pre>	<p>Configures VRRP tracking based on VLAN state transitions. You can track a combined maximum of 16 VLAN and Layer-2 interfaces.</p> <p>sub - Decreases the priority of the VRRP instance by the specified amount. When the VLAN comes up again, the value is restored to the previous priority level. Valid range is 0-255. The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the Mobility Conductor displays an error message.</p>
<pre>vrrp-master-state <vrid> add <value></pre>	<p>Specifies the VRID to use for tracking the state of the VRRP Mobility Conductor.</p> <ul style="list-style-type: none"> ■ add - Instructs the Mobility Conductor to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. Valid value is 0-255. If the priority value exceeds 255, the Mobility Conductor displays an error message similar to the following - Error: Vrrp 30 priority + tracking value exceeds 255 <p>1-255</p>
<pre>vlan</pre>	<p>Specifies the VLAN ID of the VLAN on which VRRP will run.</p> <p>1-4094</p>

Interface Tracking

You can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface. For example, interface transitions (up or down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

You must enable preempt mode to allow a managed device to take over the role of master if it detects a lower priority managed device currently acting as master

Example

The following example configures a priority of 105 for VRRP ID (VRID) 30:

```
(host) [mynode] (config) #vrrp 30
priority 105
```

The following commands configure VLAN interface tracking and assumes the following:

- You have two managed device, a primary and a backup.

- The configuration highlights the parameters for interface tracking. You may have other parameters configured for VRRP.

Primary Configuration	Backup Configuration
<pre>vrrp 10 vlan 10 ip address 10.200.22.254 priority 105 preempt tracking vlan 20 sub 10 vrrp 20 vlan 20 ip address 10.200.22.254 preempt priority 105 tracking vlan 10 sub 10 vrrp 30 vlan 30 ip address 10.200.22.254 preempt priority 105 tracking vlan 20 sub 10</pre>	<pre>vrrp 10 vlan 10 ip address 10.200.22.254 priority 100 preempt tracking vlan 20 sub 10 vrrp 20 vlan 20 ip address 10.200.22.254 preempt priority 100 tracking vlan 10 sub 10 vrrp 30 vlan 30 ip address 10.200.22.254 preempt priority 100 tracking vlan 20 sub 10</pre>

If VLAN 20 goes down, VRRP 20 automatically fails over, VRRP 10 and VRRP 30 would drop their priority to 95, causing a failover to the backup Mobility Conductor. Once VLAN 20 comes back up,

the Mobility Conductor restores the VRRP priority to 105 for all VRRP IDs and resumes the master VRRP role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

webcc

distributed
connectiontype ipv6

Description

This command changes the WebCC operational mode of a managed device from the default centralized mode to distributed mode. The WebCC operational mode determines whether the managed device or Mobility Conductor contacts the cloud WebRoot server for URL lookup queries. In the default centralized mode, the Mobility Conductor contacts the cloud WebRoot server for URL lookup queries, whereas in distributed mode, the managed device contacts the cloud WebRoot server for URL lookup queries.

The WebCC license allows all web traffic to be classified and allows the managed device to apply firewall policies based on web content category and reputation. The category and reputation data for each URL is obtained from an external WebRoot Server. The WebCC feature can operate in two distinct modes, which control whether the managed device or Mobility Conductor performs the WebCC content lookup tasks. This command can be executed only from the **/md** subtree of the Mobility Conductor.

Parameter	Description
distributed	Sets the WebCC mode for the managed device to distributed mode.
connectiontype ipv6	Sets the WebCC connection type from IPv4 to IPv6 address. The default is IPv4.

Centralized Mode

In the default **centralized** mode, only Mobility Conductor downloads the URL entry database from the WebRoot Server. If a URL for web traffic sent through the managed device does not appear in its datapath cache, the managed device sends a query request to Mobility Conductor. The Mobility Conductor queries the WebRoot Server, adds the response to its database and sends information about the URL back to the managed device.

WebCC license usage is calculated for each license pool, and the total count in each pool is sent to each managed device within that pool. If the WebCC licenses expire, or the available WebCC licenses are fewer than the AP licenses, then individual managed devices within that pool will no longer be able to send query requests to Mobility Conductor, and WebCC classification will be blocked.

If WebCC classification is blocked due to expired or insufficient licenses, individual managed devices continue to classify requested URLs currently available in the managed device datapath cache until the cache entries time out (usually over a period of 24 to 96 hours, depending upon the reputation level of the URL).

Distributed Mode

In **distributed** mode, each individual managed device downloads the complete URL entry database (approximately 22 MB) directly from the WebRoot Server. If a URL for web traffic sent through the managed device does not appear in this database, the managed device sends a query to the WebRoot Server, then adds the response to its datapath cache.

WebCC license usage is calculated for each license pool, and the total count in each pool is sent to each managed device within that pool. If the WebCC licenses expire, or the available WebCC licenses are fewer than the AP licenses, then individual managed devices within that pool will no longer be able to send new query requests to the WebRoot server. However, the WebCC feature continue to classify requested URLs that are already in the URL entry database on the managed device.

Example

The following example changes the WebCC operational mode of a managed device from the default centralized mode to distributed mode.

```
(host) [md] (config) #webcc distributed
```

Command History

Release	Modification
ArubaOS 8.4.0.0	The <code>connectiontype ipv6</code> parameter was added.
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	WebCC license.	Config mode on Mobility Conductor.

web-cc global-bandwidth-contract

```
web-cc global-bandwidth-contract
  web-cc-category <category-name> downstream|upstream kbits|mbits <bandwidth>
  web-cc-reputation high-risk|low-risk|moderate-risk|suspicious|trustworthy
  downstream|upstream kbits|mbits <1-2000>
```

Description

This command defines global bandwidth contracts for HTTP or HTTPS traffic matching a predefined web content category or reputation type.

The web content classification feature classifies all (HTTP/HTTPS) web traffic on the network. ArubaOS uses the Webroot® classification categories and risk reputation levels, URL database and URL cloud look-up service to classify the web traffic. You can create firewall policies and bandwidth contracts based upon these web traffic classification and reputation types.

Parameter	Description
web-cc-category <category-name>	Specify a web content category to apply a bandwidth contract to that category type. To see the full list of available web content categories, issue the command <code>show web-cc categories</code> .
downstream upstream	Specify downstream to apply the bandwidth contract to downstream traffic from the Mobility Conductor. Specify upstream to apply the contract to upstream traffic to the Mobility Conductor.
kbits mbits	Select kbits to define the contract bandwidth in kilobits/second. Select mbits to define the contract in megabits/second.
bandwidth	Define the contract value, If you are defining the bandwidth value in kilobits/second, the supported range is 256-2,000,000 kbits. If you are defining the bandwidth value in megabits/second, the supported range is 1-2000 mbits. 256-2,000,000 kbits 1-2000 mbits
web-cc-reputation high-risk low-risk moderate-risk suspicious trustworthy	Define a bandwidth contract for traffic associated with one of five predefined reputation types. Session ACLs can be applied to these risk categories using the <code>ip access-list session</code> command.

Example

The following example creates a 100 megabit/second bandwidth contract for a category called **music**:

```
(host) [/md] (config) #web-cc global-bandwidth-contract web-cc-category
music downstream mbits 100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	WebCC license.	Config mode on Mobility Conductor.

web-proxy server

```
web-proxy server <name>  
    port
```

Description

This command configures the web-proxy server related information.

When the Mobility Conductor needs to access data on the cloud or the internet, and if the internet bound traffic needs to pass through a proxy, execute the `web-proxy server` command. Once the command is executed the Mobility Conductor routes web (HTTP/HTTPS) traffic through the proxy server.

Parameter	Description
<name>	Specifies the proxy server name / IP address.
port	Specifies the proxy server port.

Example

The following example configures the web-proxy server related information:

```
(host) [mynode] (config) #web-proxy server arubaproxy.com port 8080
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

web-server profile

```
web-server profile
  absolute-session-timeout <30-3600>
  bypass-cp-landing-page
  captive-portal-cert <name>
  ciphers {high|low|medium}
  cipher-suite <cipher(s)>
  exclude-http-security-headers
  idp-cert <idp-cert>
  mgmt-auth [certificate] [username/password]
  no ...
  session-timeout <session-timeout>
  ssl-protocol [tlsv1 | tlsv1.1 | tlsv1.2]
  switch-cert <name>
  via-client-cert-port <via-client-cert-port>
  web-https-port-443
  web-max-clients <web-max-clients>
```

Description

This command configures the Mobility Conductor's web server.

There is a default server certificate installed in the Mobility Conductor, However this certificate does not guarantee security in production networks. Best practices are to replace the default certificate with a custom certificate issued for your site by a trusted CA. See the *ArubaOS User Guide* for more information about how to generate a CSR to submit to a CA and how to import the signed certificate received from the CA into the Mobility Conductor. After importing the signed certificate into the Mobility Conductor, use the `web-server profile` command to specify the certificate for captive portal or WebUI access. If you need to specify a different certificate for captive portal or WebUI access, use the `no` command to revert back to the default certificate before you specify the new certificate (see the Example section).

You can use client certificates to authenticate management users. If you specify certificate authentication, you need to configure certificate authentication for the management user with the `mgmt-user webui-cacert` command.

Parameter	Description
<code>absolute-session-timeout</code> <code><30-3600></code>	Specifies the absolute time after which the WebUI session times out post a successful authentication. 30-3600 seconds 0 (disabled)

Parameter	Description
bypass-cp-landing-page	<p>If disabled, the Mobility Conductor uses the new redirection scheme also known as the landing page by default including the meta tag. This can reduce the CPU load on the Mobility Conductor. The Mobility Conductor falls back to the old redirection scheme if this parameter is enabled.</p> <p>disabled</p>
captive-portal-cert	<p>Specifies the name of the server certificate associated with captive portal. Use the <code>show crypto-local pki ServerCert</code> command to see the server certificates installed in the Mobility Conductor.</p> <p>default</p>
ciphers	<p>Configures the strength of the cipher suite: high: encryption keys larger than 128 bits low: 56 or 64 bit encryption keys medium: 128 bit encryption keys This command is not available in FIPS software images because ciphers are pre-configured only to acceptable values. high, low, medium Default: high This parameter is available only for ArubaOS 8.10.0.0 and versions prior to that.</p>
cipher-suite <cipher(s)>	<p>Enables cipher suites. Default: GCM encryption based cipher suites. Starting from 8.11.0.0, specific cipher suites can be enabled from the list of supported ciphers suites.</p>
exclude-http-security-headers	<p>Excludes security headers from HTTP response.</p>
idp-cert	<p>Specifies the IDP certificate name configured in the Mobility Conductor.</p>
mgmt-auth	<p>Specifies the authentication method for the management user; you can choose to use either username or password or certificates, or both username or password and certificates. username/password, certificate username/password</p>
no	<p>Negates any configured parameter.</p>

Parameter	Description
<pre>session-timeout <session-timeout></pre>	<p>Specifies the time of inactivity after which the WebUI session times out and requires login for continued access.</p> <p>30-3600 seconds 900 seconds</p>
<pre>ssl-protocol</pre>	<p>Specifies the SSL or TLS protocol version used for securing communication with the web server:</p> <ul style="list-style-type: none"> ■ TLS v1 ■ TLS v1.1 ■ TLS v1.2 <p>Default: tlsv1.2</p>
<pre>switch-cert</pre>	<p>Specifies the name of the server certificate associated with WebUI access. Use the <code>show crypto-local pki ServerCert</code> command to see the server certificates installed in the Mobility Conductor.</p> <p>default</p>
<pre>via-client-cert-port <via-client-cert-port></pre>	<p>Configures a port for VIA client certificate-based authentication.</p>
<pre>web-https-port-443</pre>	<p>Enables WebUI access on the HTTPS port (443). When you connect to the WebUI using https (tcp port 443), the Mobility Conductor continues using port 443 and no longer redirects to port 4343.</p>
<pre>web-max-clients <web-max-client></pre>	<p>Configures the web server's maximum number of supported concurrent clients.</p> <p>25-320 75</p>

Example

The following example configures the Mobility Conductor's web server:

```
(host) [/md] (config) #web-server profile
absolute-session-time.. Configure user's absolute WebUI session timeout
<30-3600> (seconds)
bypass-cp-landing-page Enable bypass captive portal landing page
captive-portal-cert Server Certificate for Captive Portal
cipher-suite<cipher(s)> Enable cipher suites. GCM encryption based cipher
suites are default
exclude-http-security.. Exclude security headers from HTTP response
```

```

idp-cert                Server Certificate for IDP
mgmt-auth               Configure management user's WebUI access method,
either
username/password authentication or certificate
authentication or both. Default is username/password
authentication
no                       Delete Command
session-timeout         Configure user's WebUI session timeout <30-3600>
(seconds)
ssl-protocol            Configure SSL/TLS protocol. Default is TLSv1.2.
switch-cert            Server Certificate for Management WebUI
via-client-cert-port    Port number used for VIA client-cert based profile
download. Valid range is <1025-65535>. Default value is
8085
web-https-port-443     Enable WebUI access on HTTPS port (443)
web-max-clients         Configure web servers' maximum supported concurrent
clients <25-320>

```

The following example configures WebUI access with client certificates only, and specify the server certificate for the Mobility Conductor:

```

(host) [/md] (config) #web-server profile
(host) [/md] (Web Server Configuration) #mgmt-auth certificate
(host) [/md] (Web Server Configuration) #switch-cert ServerCert1
(host) (Web Server Configuration) #!
(host) [/md] (config) #mgmt-user webui-cacert test_string serial 1111 admin
root

```

To specify a different server certificate, use the `no` command to revert back to the default certificate *before* you specify the new certificate:

```

(host) [/md] (config) #web-server profile
(host) [/md] (Web Server Configuration) #mgmt-auth certificate
(host) [/md] (Web Server Configuration) #switch-cert ServerCert1
(host) [/md] (Web Server Configuration) #no switch-cert
(host) [/md] (Web Server Configuration) #switch-cert ServerCert2

```

Command History

Release	Modification
ArubaOS 8.11.0.0	The cipher-suite <cipher(s)> parameter was introduced. The ciphers parameter was removed.
ArubaOS 8.7.0.0	TLS v1.2 is the default ssl-protocol in the Web-Server. TLS v1 and TLS v1.1 is disabled by default.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The <code>web-server ciphers</code> and <code>web-server ssl-protocol</code> commands require the PEFNG license.	Config mode on Mobility Conductor.

websocket clearpass

```
websocket clearpass
  enable
  no
  primary host <host> port <1-65535> username <username> passwd <passwd>
  secondary host <host> port <1-65535> username <username> passwd <passwd>
```

Description

This command configures the ClearPass WebSocket profile. This command configures the primary and secondary ClearPass Insight server.

Parameter	Description
enable	Enable ClearPass WebSocket interface.
no	Remove or negate a parameter.
primary	Configure the primary ClearPass Insight server. This parameter has the following sub-parameters: <ul style="list-style-type: none">■ host-The primary ClearPass Insight server IP address.■ port-The port number of the ClearPass Insight server.■ username- The name of the user who can perform the action on the server.■ passwd- The password of the user. port: 1-65535 username: 1-255 bytes password: 6-100 bytes port: 443
secondary	Configure the secondary ClearPass Insight server. This parameter has the following sub-parameters: <ul style="list-style-type: none">■ host-The primary ClearPass Insight server IP address.■ port-The port number of the ClearPass Insight server.■ username- The name of the user who can perform the action on the server.■ passwd- The password of the user. port: 1-65535 username: 1-255 bytes password: 6-100 bytes port: 443

Example

The following example configures the ClearPass WebSocket interface and the primary and secondary ClearPass Insight server:

```
(host) [mynode] (config) #websocket clearpass
(host) [mynode] (ClearPass WebSocket Profile) #primary host
security67.acmecompany.com port 443 username admin passwd changeme
(host) [mynode] (ClearPass WebSocket Profile) #secondary host 10.17.5.210
port 443 username aosadmin passwd changeme
(host) [mynode] (ClearPass WebSocket Profile) #enable
(host) [mynode] (ClearPass WebSocket Profile) #write memory

Saving Configuration...
Partial configuration for (root) /:
-----
Contents of : /flash/config/partial/143/p=.cfg
websocket clearpass
enable
primary host "security67.acmecompany.com" port 443 username "admin" passwd
"changeme"
secondary host "10.17.5.210" port 443 username "aosadmin" passwd "changeme"
!
Partial configuration for /mynode:
-----
Contents of : /flash/config/partial/143/p=mynode.cfg
websocket clearpass
enable
primary host "security67.acmecompany.com" port 443 username "admin" passwd
"changeme"
secondary host "10.17.5.210" port 443 username "aosadmin" passwd "changeme"
!
Configuration Saved.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

whoami

whoami

Description

This command displays information about the current user logged into the Mobility Conductor or managed device. Use this command to display the name and role of the user who is logged into the device for this session.

Example

The following example displays information about the user logged into the Mobility Conductor:

```
(host) [node] (config) #whoami
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Conductor.

wipe

wipe out flash

Description

This command erases all data including configuration, logs, license keys, flash backup files and formats the flash file system in the controller. This command can also be used to return the Mobility Conductor or the managed devices to the factory default state. After issuing the command and rebooting the controller, you can return the controller to an operational state by installing the ArubaOS image again.



Issue this command only when the controller is taken out of service or decommissioned.

Example

The following example formats the flash file system:

```
(host) #wipe out flash
Do you really want to wipe out the entire flash (y/n): y
Zeroing out flash:.....
Flash zeroed out successfully.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Conductor.

wlan 6ghz-rrm-ie-profile

```
wlan 6ghz-rrm-ie-profile <profile-name>
  bss-aac-ie-6ghz
  clone
  country-ie-6ghz
  enabled-capabilities-ie-6ghz
```

```
no
pwr-constraint-ie-6ghz
qbss-load-ie-6ghz
quiet-ie-6ghz
tpc-report-ie-6ghz
```

Description

This command configures a Radio Resource Management (RRM) Information Elements (IE) profile to define the information elements advertised by a Wi-Fi 6E AP for 6 GHz band. ArubaOS supports RRM IEs for Wi-Fi 6E APs with 802.11ax support enabled. All IEs are sent by default.

Parameter	Description
bss-aac-ie-6ghz	The AP advertises the BSS Available Admission Capacity IE in beacon and probe responses for 6 GHz band. The BSS Available Admission Capacity IE contains information about the admission capabilities for each User Priority or AC.
clone	Copy the settings of an existing RRM IE profile for 6 GHz band.
country-ie-6ghz	The AP advertises the device's regulatory domain in beacon and probe responses.
enabled-capabilities-ie-6ghz	The AP advertises support for radio measurements in a device in beacon and probe responses for 6 GHz band.
no ...	Disables the transmission of an IE in this profile.
pwr-constraint-ie-6ghz	The AP advertises the regulatory maximum transmit power for that current channel in beacon and probe responses for 6 GHz band.
qbss-load-ie-6ghz	The AP advertises the QBSS Load IE in beacon and probe responses for 6 GHz band. The QBSS Load IE contains information on the current station count, channel utilization, and available admission capacity levels in the QBSS.
quiet-ie-6ghz	The AP advertises the Quiet IE in beacon and probe responses for 6 GHz band. Quiet IE is used to silence the channel for measurement purposes. When an AP uses a Quiet IE to schedule a quiet interval, stations may not transmit on that channel during the quiet interval.
tpc-report-ie-6ghz	The AP advertises information about its TCP in beacon and probe responses for 6 GHz band.

Example

The following example allows the Wi-Fi 6E AP to advertise the country IE.

```
(host) [md] (config) #wlan 6ghz-rrm-ie-profile default
(host) [md] (RRM IE Profile for 6 GHz "default") #country-ie-6ghz
```

Command History

Release	Description
ArubaOS 8.9.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan anyspot-profile

```
wlan anyspot-profile <profile-name>
  clone <profile-name>
  enable-anyspot
  exclude-ssid <exclude-ssid>
  exclude-wildcard <exclude-wildcard>
  no
  preset-ssid <preset-ssid>
```

Description

The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.

When an AP is configured to use this feature, the anyspot AP radio hides its configured ESSID in beacons, and compiles a list of other ESSIDs from detected neighboring APs. If the client sends a probe request without a specified ESSID, the anyspot AP will respond with a preconfigured ESSID.

When a client searches for a preferred network, that client sends the SSID of the preferred network in the probe request. The anyspot AP checks to see if there is a neighboring AP using that ESSID that can respond the client's request. If no matching network is found, the anyspot AP sends a response to the client using the SSID from the client request. If the client is authorized to connect to the anyspot AP, that client associates to AP. Once connected to the anyspot AP, the client recognizes the ESSID to which it is connected as one associated with its preferred network, and does not send out any further probe requests.

Parameter	Description
<code>clone <profile-name></code>	Make a copy of an existing anyspot profile.
<code>enable-anyspot</code>	Issue this command to enable the anyspot feature. Note that you must associate the anyspot profile with a virtual AP profile for the settings to take effect.
<code>exclude-ssid <exclude-ssid></code>	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the Exclude ESSID lists. To add an ESSID to the list, enter the full name of the ESSID, then click Add . To remove an ESSID from the list, select it and click Delete . ESSIDs from neighboring APs will automatically appear in this list as long as the anyspot-enabled AP can detect that ESSID.
<code>exclude-wildcard <exclude-wildcard></code>	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the Exclude ESSID list. To exclude ESSIDs that partially match a text string, enter that string then click Add . To remove a matching string from the list, select it and click Delete .

Parameter	Description
no	Remove or negate any configured parameter.
preset-ssid <preset-ssid>	The anyspot-enabled AP will not send an ESSID in beacons, but if a client sends a probe request without an ESSIDs (that is, the probe request is not looking for a specific network) then the anyspot-enabled AP will respond to the probe request with an ESSID from this list.

Example

The following example defines a ESSID to be returned in probe requests that do not contain an ESSID, as well as two ESSIDs that should be excluded from anyspot responses, in the event that a client is probing for one of these excluded ESSIDs.

```
(host) [/md] (config) #wlan anyspot-profile anyspot1
(host) [/md] (Anyspot profile "anyspot1") #preset SSID companyguest
(host) [/md] (Anyspot profile "anyspot1") #exclude-ssid corp_dev_essid
(host) [/md] (Anyspot profile "anyspot1") #exclude-ssid corp_voip_essid
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan bcn-rpt-req-profile

```
wlan bcn-rpt-req-profile <profile-name>
  bssid <bssid>
  channel <channel>
  clone <source>
  include-ssid
  interface <interface>
  last-beacon-rpt-indication
  measure-dur-mandatory
  measure-duration <measure-duration>
  measure-mode
  no
  random-interval <random-interval>
  reg-class {auto|1|12|81|115|131}
  request-info <request-info>
  rpt-condition <rpt-condition>
  rpt-detail
  ssid <ssid>
```

Description

Configures a Beacon Report Request Profile to provide the parameters for the Beacon Report Request frames. The Beacon Report Request profile is configured under the 802.11K profile.

Parameter	Description
<profile-name>	Name of this instance of the profile. The name must be 1-63 characters. "default
bssid <bssid>	BSSID included in the beacon request. wildcard
channel <channel>	This option is used to set the Channel field in the Beacon Report Request frame. The Channel value can be set to one of the following: <ul style="list-style-type: none">■ The channel of the AP (when Measurement Mode is set to either 'Passive' or 'Active-All channels')■ 0 (when Measurement Mode is set to 'Beacon Table')■ 255 (when Measurement Mode is set to 'Active-Channel Report') For 802.11b/g band: 1 to 14 For 802.11a band: 36 to 165 255

Parameter	Description
clone <source>	Creates a copy of the Beacon Report Request Profile specified as the <source>. <source> is the name of an existing Beacon Report Request Profile from which parameter values are copied.
include-ssid	Include SSID IE in Beacon Report Request. Enable
interface <interface>	This field is used to specify the radio interface for transmitting the Beacon Report Request frame. 0-1 1
last-beacon-rpt-indication	Enable Last Beacon Request Indication sub-element in Beacon Report Request. Disable
measure-dur-mandatory	This value is used to set the Duration Mandatory bit of the Measurement Request Mode field of the Beacon Report Request frame. Disabled
measure-duration <measure-duration>	This value is used to set the Measurement Duration field in the Beacon Report Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs. 0 – 65535 0
measure-mode	Indicates the mode used for the measurement. The valid measurement modes are: <ul style="list-style-type: none"> ■ active-all-ch—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ active-ch-rpt—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ■ beacon-table—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ■ passive—Enables passive beacon measurement

Parameter	Description
	<p>mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report.</p> <p>NOTE: If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table</p> <p>beacon-table</p>
no	Negates any configured parameter.
<pre>random-interval <random-interval></pre>	<p>This value is used to set the Randomization Interval field in the Beacon Report Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units). A Randomization Interval of 0 in a measurement request indicates that no random delay is to be used.</p> <p>0 – 65535</p> <p>0</p>
<pre>reg-class {auto 1 12 81 115 131}</pre>	<p>This option is used to specify the Regulatory Class field in the Beacon Report Request frame.</p> <p>Range: auto, 1, 12, 81, 115, 131</p> <p>Default: auto</p> <p>For 802.11b/g bands, use 12.</p> <p>For 802.11a band, use 1</p> <p>Auto uses value based on country code.</p>
<pre>request-info <request-info></pre>	<p>This option is used to indicate the contents of the Request Information IE that could be present in the Beacon Report Request frame. The Request Information IE is present for all Measurement Modes except the Beacon Table mode. It consists of a list of Element IDs that should be included by the client in the response frame.</p> <p>Any valid element ID in the x/y/z format. For example, 0/21/22.</p>
<pre>rpt-condition <rpt-condition></pre>	<p>This option is used to indicate the value for the Reporting Condition field in the Beacon Reporting Information sub-element present in the Beacon Report Request frame.</p> <p>0 - 255</p> <p>0</p>

Parameter	Description
rpt-detail	This option is used to indicate the value for the Detail field in the Reporting Detail sub-element present in the Beacon Report Request frame. Disabled
ssid <ssid>	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN- 01).

Example

The following example configures the parameters under **bcn-rpt-req-profile**.

```
(host) [/md] (config) #wlan bcn-rpt-req-profile default
(host) [/md] (Beacon Report Request Profile "default") #channel 9
(host) [/md] (Beacon Report Request Profile "default") #interface 1
(host) [/md] (Beacon Report Request Profile "default") #no measure-dur-
mandatory
(host) [/md] (Beacon Report Request Profile "default") #measure-duration
100
(host) [/md] (Beacon Report Request Profile "default") #measure-mode
active-all-ch
(host) [/md] (Beacon Report Request Profile "default") #random-interval 100
(host) [/md] (Beacon Report Request Profile "default") #reg-class 12
(host) [/md] (Beacon Report Request Profile "default") #rpt-condition 2
(host) [/md] (Beacon Report Request Profile "default") #no rpt-detail
(host) [/md] (Beacon Report Request Profile "default") #request-info
0/21/22
(host) [/md] (Beacon Report Request Profile "default") #ssid aruba-ap
```

Command History

Release	Modification
ArubaOS 8.9.0.0	The values auto , 81 , 115 , and 131 were introduced for the <code>reg-class</code> parameter.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan client-wlan-profile

```
wlan client-wlan-profile <profile-name>
auth-as-computer
auth-as-guest
clone
eap-cert
eap-cert-connect-only-to
eap-peap
eap-peap-connect-only-to
eap-type
enable-8021x
ieap-cert-connect-only
inner-eap
inner-eap-type
no
non-broadcasting-connection
range-connect
ssid-profile
```

Description

You can push WLAN profiles to users computers that use the Microsoft Windows Wireless Zero Config (WZC) service to configure and maintain their wireless networks. After the WLAN profiles are pushed to user computers, they are automatically displayed as an ordered list in the preferred networks.

Parameter	Description
auth-as-computer	Authenticate with domain credentials.
auth-as-guest	Authenticate as a guest user.
clone	Copy settings from another WLAN client profile.
eap-cert	If you select EAP type as certificate, you can use one of the following options: <ul style="list-style-type: none">■ use-smartcard■ simple-certificate-selection■ use-different-name■ validate-server-certificate
eap-cert-connect-only-to	Comma separated list of servers.
eap-peap	Configure one of the following EAP-PEAP settings: <ul style="list-style-type: none">■ disconnect-if-no-crypto■ dont-allow-user-authorize■ enable-fast-reconnect■ enable-quarantine-checks

Parameter	Description
	<ul style="list-style-type: none"> ■ validate-server-certificate
eap-peap-connect-only-to	Comma separated list of servers.
eap-type	<p>Select one of the following EAP types used by the client to connect to wireless network:</p> <ul style="list-style-type: none"> ■ eap-peap - Select this option to specify EAP-PEAP as the authentication protocol. ■ eap-tls - Select this option to specify EAP-TLS as the authentication protocol. <p>EAP-PEAP</p>
enable-8021x	<p>Select this option to enable 802.1X authentication for this network.</p> <p>Enabled</p>
ieap-cert-connect-only-to	Command separated list of servers that the Inner EAP Certificates connects to.
inner-eap	<p>Enter the inner EAP type.</p> <p>EAP-MSCHAPv2</p>
inner-eap-type	<p>Specify one of the following:</p> <ul style="list-style-type: none"> ■ eap-gtc - Select this option to specify EAP-GenericTokenCard as the inner authentication protocol. ■ eap-mschapv2 - Select his option to specify EAP-MSCHAPV2 as the inner authentication protocol.
no	Negate and reset all configuration settings.
non-broadcasting-connection	<p>Connect even if WLAN is not broadcasting.</p> <p>Disabled</p>
range-connect	Automatically connect to this WLAN if in range.
ssid-profile	Enter the name of the SSID profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan dot11k-profile

```
wlan dot11k <profile-name>
  ap-chan-rpt-11a <ap-chan-rpt-11a>
  ap-chan-rpt-11bg <ap-chan-rpt-11bg>
  ap-chan-rpt-6ghz <ap-chan-rpt-6ghz>
  bcn-measurement-mode {active-all-ch|active-ch-rpt|beacon-table|passive}
  bcn-req-chan-11a <bcn-req-chan-11a>
  bcn-req-chan-11bg <bcn-req-chan-11bg>
  bcn-req-time <bcn-req-time>
  bcn-rpt-req-profile <profile-name>
  clone <profile-name>
  dot11k-enable
  force-disassoc
  lm-req-time <lm-req-time>
  nb-resp-wide-band-ie
  no ...
  rrm-ie-profile <profile-name>
  tsm-req-profile <profile-name>
  tsm-req-time <tsm-req-time>
```

Description

This command configures a 802.11k radio profile. In a 802.11k network, if the AP with the strongest signal is reaches its maximum capacity, clients may connect to an under utilized AP with a weaker signal. A 802.11k profile can assigned to each virtual AP.

Parameter	Description
<profile-name>	Name of this instance of the profile. 1-63 characters default
ap-chan-rpt-11a <ap-chan-rpt-11a>	This value is sent in the Channel field of the AP channel reports on the 'A' radio. 34-165 36
ap-chan-rpt-11bg <ap-chan-rpt-11bg>	This value is sent in the Channel field of the AP channel reports on the 'BG' radio. 1-14 1
ap-chan-rpt-6ghz <ap-chan-rpt-6ghz>	This value is sent in the Channel field of the AP channel reports on the 6 GHz radio. 1-233 1

Parameter	Description
bcn-measurement-mode	<p>Configures a beacon measurement mode for the profile.</p> <ul style="list-style-type: none"> ■ active-all-ch—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ active-ch-rpt—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ■ beacon-table—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ■ passive—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. <p>NOTE: If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table</p> <p>beacon-table</p>
beacon-table	<p>Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode.</p> <p>NOTE: If a station doesn't support beacon-table measurement mode, it returns a Beacon Measurement Report with the <i>Incapable</i> bit set in the <i>Measurement Report Mode</i> field.</p>

Parameter	Description
passive	<p>Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report.</p> <p>NOTE: If a station doesn't support passive measurement mode, it returns a Beacon Measurement Report with the <i>Incapable</i> bit set in the <i>Measurement Report Mode</i> field.</p>
clone <profile-name>	Copy settings from another specified 802.11k profile.
bcn-req-chan-11a <bcn-req-chan-11a>	<p>This value is sent in the Channel field of the beacon requests on the 'A' radio.</p> <p>34 to 165</p>
bcn-req-chan-11bg <bcn-req-chan-11bg>	<p>This value is sent in the Channel field of the Beacon Requests on the BG radio.</p> <p>1 to 14 or 0 to 255</p>
bcn-req-time <bcn-req-time>	<p>This option configures the time duration between two consecutive beacon requests sent to a802.11k client. By default, the beacon requests are sent to a802.11k client every 60 seconds. However, if a different value is required, the <code>bcn-req-time</code> option can be used.</p> <p>10-200 seconds 60 seconds</p>
bcn-rpt-req-profile <profile-name>	Beacon Report Request Settings for the selected profile.
dot11k-enable	<p>Enables the 802.11K feature. This feature is disabled by default.</p> <p>Disabled</p>
force-dissasoc	<p>This feature allows the AP to forcefully disassociate on-hook voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its CAC limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfill their QoS requirements.</p>

Parameter	Description
	<p>NOTE: This feature is disabled by default.</p> <p>Disabled</p>
<code>lm-req-time <lm-req-time></code>	<p>This option configures the time duration between two consecutive link measurement requests sent to an 802.11k client. By default, link measurement requests are sent to a 802.11k client every 61 seconds. However, you can use the <code>lm-req-time</code> option to specify different time interval.</p> <p>10 to 200 seconds 60 seconds</p>
<code>nb-resp-wide-band-ie</code>	<p>Includes the wide channel bandwidth information element in the neighbor report responses, when the dot11k setting is enabled on the managed device.</p>
<code>no</code>	<p>Negates or removes any configured parameter.</p>
<code>rrm-ie-profile <profile-name></code>	<p>RRM IE Settings Profile.</p>
<code>tsm-req-profile <profile-name></code>	<p>TSM Report Request Settings Profile.</p>
<code>tsm-req-time <tsm-req-time></code>	<p>This option configures the time duration between two consecutive transmit stream measurement requests sent to a 802.11k client. By default, the transmit stream measurement requests are sent to a 802.11k client every 90 seconds. However, you can use the <code>tsm-req-time</code> option to specify a different time interval.</p> <p>10 seconds to 200 seconds. 90 seconds</p>

Example

The following example enables the 802.11k feature on the 802.11k profile and configures the beacon measurement mode and specifies the time interval for beacon, link, and transmit stream measurement requests.

```
(host) [/md] (config) #wlan dot11k-profile default
(host) [/md] (802.11K Profile "default") #dot11k-enable
(host) [/md] (802.11K Profile "default") #bcn-measurement-mode beacon-table
(host) [/md] (802.11K Profile "default") #bcn-req-time 60
```



```
(host) [/md] (802.11K Profile "default") #lm-req-time 60
(host) [/md] (802.11K Profile "default") #tsm-req-time 90
```

Related Command

Command	Description
wlan rrm-ie-profile	Configure a radio resource management RRM IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.10.0.0	The <code>nb-resp-wide-band-ie</code> parameter was added.
ArubaOS 8.9.0.0	The <code>ap-chan-rpt-6ghz</code> parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan dot11r-profile

```
wlan dot11r-profile <profile-name>  
  clone  
  dot11r  
  key-duration <60-86400>  
  key-assignment  
  mob-domain-id <1-65535>  
  no
```

Description

This command configures an 802.11r radio profile. You can enable and configure Fast BSS Transition on a per Virtual AP basis. You must create an 802.11r profile and associate that with the Virtual AP profile through an SSID profile.

Parameter	Description
<profile-name>	Name of this instance of the profile. 1-63 characters Default
clone	Name of an existing dot11r-profile from which the parameter values are copied.
mob-domain-id	An ID that uniquely identifies the mobility domain. 1-65535 1
dot11r	Enables the Fast BSS Transition capability. Disabled
no	Negates or removes any configured parameter.
key-duration	The r1 key timeout value in seconds for decrypt-tunnel or bridge mode. 60-86400 3600
key-assignment	The list of neighbor APs for decrypt-tunnel or bridge mode. <ul style="list-style-type: none">■ static: Get neighbor AP list from ARM or VBR.■ dynamic: Use all APs from ap-group as the neighbor list.

Example

The following examples enable the 802.11r capability on the 802.11r profile, configures the Fast BSS mobility domain ID, and specifies the r1 key time-out value.

```
(host) [/md] (config)#wlan dot11r-profile default
(host) [/md] (802.11r Profile "default") #fastbss-transition
(host) [/md] (802.11r Profile "default") #fastbss-mob-domain-id 25
(host) [/md] (802.11r Profile "default") #r1key_validity_duration 2500
```

Configure a mobility domain ID that uniquely identifies a mobility domain using the following command:

```
(host) [mynode] (802.11r Profile "default") #mob-domain-id <1-65535>
```

The default value is 1.

Configure the r1 key timeout value in seconds for decrypt-tunnel or bridge mode using the following command:

```
(host) [mynode] (802.11r Profile "default") #key_duration <60-86400>
```

The default value is 3600 seconds.

Apply the 802.11r profile to an SSID profile using the following command:

```
(host) [mynode] (config) #wlan ssid-profile voice dot11r-profile voice-enterprise
```

You can advertise the 802.11r capability on the Virtual AP profile by applying the SSID profile. Use the following command to apply the SSID profile to the Virtual AP profile:

```
(host) [mynode] (config) #wlan virtual-ap voice-AP ssid-profile voice
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan edca-parameters-profile

```
wlan edca-parameters-profile
  ap|station <profile-name>
    background [acm <0-1>|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]][txop
    <0-2047>]
    best-effort [acm <0-1>|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]][txop
    <0-2047>]
    clone <source>
    no
    video [acm <0-1>|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]][txop <0-
    2047>]
    voice [acm <0-1>|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]][txop <0-
    2047>]
```

Description

This command configures an EDCA profile for APs or for clients (stations).

EDCA profiles are specific either to APs or clients. You apply an EDCA profile to a specific SSID profile. Use this command only under the guidance of your Aruba technical support representative.

Parameter	Description
<profile-name>	Name of this instance of the profile. 1-63 default
background	Configures the background queue.
best-effort	Configures the best-effort queue.
clone	Name of an existing EDCA profile from which parameter values are copied.
no	Remove or negate a parameter.
video	Configures the video queue.
voice	Configures the voice queue.
acm	Specifies mandatory admission control. The client reserves the AC through TSPEC signaling. 0-disable, 1-enable 0
aifsn	Arbitrary inter-frame space number.

Parameter	Description
	0-15 0
ecw-max	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1 . A value of 4 computes to $2^4-1 = 15$. 0-15 0
ecw-min	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1 . A value of 4 computes to $2^4-1 = 15$. 0-15 0
txop	TXOP in units of 32 microseconds. Divide the desired transmission duration by 32 to determine the value to configure. For example, for a transmission duration of 3008 microseconds, enter 94 (3008/32). 0-2047 0

The following are the default values configured for APs:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	6	3	0	No
background	4	10	7	0	No
video	3	4	1	94	No
voice	2	3	1	47	No

The following are the default values configured for clients:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	10	3	0	No
background	4	10	7	0	No
video	3	4	2	94	No
voice	2	3	2	47	No

Example

The following example configures an EDCA profile for APs:

```
(host) [/md] (config) #wlan edca-parameters-profile ap edca1
(host) [/md] (EDCA Parameters profile (AP) "edca1") #best-effort ecw-min 15
ecw-max 15 aifsn 15 txop 100 acm 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Conductor

wlan he-ssid-profile

```
wlan he-ssid-profile <profile-name>
  clone
  dynamic-fragmentation-level <dynamic-fragmentation-level>
  he-duration-based-rts <he-duration-based-rts>
  he-guard-interval
  he-mu-mimo
  he-mu-ofdma
  he-supported-mcs-map <he-supported-mcs-map>
  he-ul-mu-mimo
  he-txbf
  high-efficiency-enable
  individual-twt
  no...
```

Description

This command configures a high-efficiency SSID profile.

Parameter	Description
<profile-name>	Name of this instance of the profile. 1-63 characters default
clone	Name of an existing high-efficiency SSID profile from which parameter values are copied.
dynamic-fragmentation-level	Controls the level of dynamic fragmentation that is supported by the APs. Enter one of the following values: <ul style="list-style-type: none">0: Does not support Dynamic Fragmentation1: Support for dynamic fragments that are contained within an S-MPDU. It does not support dynamic fragment within an A-MPDU that is not an S-MPDU.2: Support for dynamic fragments that are contained within an S-MPDU, and support for up to one dynamic fragment for each MSDU within an A-MPDU.3: Support for dynamic fragments that are contained within an S-MPDU, and support for up to four dynamic fragments for each MSDU within an A-MPDU. 0-3 0
he-duration-based-rts	Indicates the duration-based RTS value, in microseconds, in the HE capability. When the Transmission Opportunity (TXOP) is greater than the configured duration-based RTS value, RTS/CTS exchange value is used. 0-1023

Parameter	Description
	1023
he-guard-interval	Sets the supported GI. 800 ns, 1600 ns, 3200 ns 800
he-mu-mimo	Enables or disables HE MU-MIMO in WLAN high-efficiency SSID. enabled
he-mu-ofdma	Enables or disables HE MU-OFDMA in WLAN high-efficiency SSID. enabled
he-supported-mcs-map	Comma separated list of maximum supported MCS for spatial streams 1 through 8. Valid values for maximum MCS are 7, 9, 11, and '-' (if spatial stream is not supported). Maximum MCS of a spatial stream cannot be higher than the previous streams. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it is not used for Tx and Rx. 7,9,11, - 11,11,11,11,11,11,11,11
he-ul-mu-mimo	Enables uplink MU-MIMO in HE capability. NOTE: Only AP-535 and AP-555 access points support uplink MU-MIMO transmission.
he-txbf	Enables or disables Transmit Beamforming (TxBF) in HE capability. enabled
high-efficiency-enable	Enables or disables high-efficiency (802.11ax) features in SSID. enabled
individual-twt	Enables or disables individual TWT support. enabled
no	Negates any configured parameter.

Example

The following example configures the dynamic fragmentation level supported by the AP for the default high-efficiency SSID:


```
(host) [md] (config) #wlan he-ssid-profile default
(host) [md] (High-efficiency SSID profile "default") #dynamic-fragmentation-
level 2
```

Command History

Release	Modification
ArubaOS 8.8.0.0	The <code>he-ul-mu-mimo</code> parameter was introduced.
ArubaOS 8.6.0.0	The following parameters were added: <code>he-mu-mimo</code> <code>he-mu-ofdma</code> <code>high-efficiency-enable</code>
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All 802.11 ax capable APs.	Base operating system	Config mode on Mobility Conductor.

wlan hotspot advertisement-profile

```
wlan hotspot advertisement profile <profile-name>
  anqp-3gpp-nwk-profile <profile-name>
  anqp-domain-name-profile <profile-name>
  anqp-ip-addr-avail-profile <profile-name>
  anqp-nai-realm-profile <profile-name>
  anqp-nwk-auth-profile <profile-name>
  anqp-roam-cons-profile <profile-name>
  anqp-venue-name-profile <profile-name>
  clone <profile-name>
  h2qp-conn-cap-profile <profile-name>
  h2qp-op-cl-profile <profile-name>
  h2qp-operator-friendly-profile <profile-name>
  h2qp-osu-prov-list-profile <profile-name>
  h2qp-wan-metrics-profile <profile-name>
  no
  osu-ssid
```

Description

This command configures a WLAN advertisement profile for an 802.11u public access service provider.

Hotspot 2.0 is a WFA specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

Access Network Query Protocol (ANQP) and Hotspot 2.0 Query Protocol (H2QP) profiles define the information in the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP and H2QP profile to be associated with the advertisement profile.

Values configured in the ANQP profiles will not be sent to clients unless you:

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<code>anqp-3gpp-nwk-profile <profile-name></code>	Name of the Access Network Query Protocol (ANQP) 3GPP cellular network profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-3gpp-nwk-profile on page 4139 .

Parameter	Description
anqp-domain-name-profile <profile-name>	Name of the ANQP domain name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-domain-name-profile on page 4141 .
anqp-ip-addr-avail-profile <profile-name>	Name of the ANQP IP Address Availability profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-ip-addr-avail-profile on page 4143 .
anqp-nai-realm-profile <profile-name>	Name of the ANQP NAI Realm profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-nai-realm-profile on page 4145 .
anqp-nwk-auth-profile <profile-name>	Name of the ANQP Network Authentication profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-nwk-auth-profile on page 4150 .
anqp-roam-cons-profile <profile-name>	Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-roam-cons-profile on page 4152 .
anqp-venue-name-profile <profile-name>	Name of the ANQP Venue Name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-venue-name-profile on page 4154 .
clone <profile-name>	Make a copy of an existing WLAN Advertisement profile.

Parameter	Description
h2qp-conn-cap-profile <profile-name>	Name of the Hotspot 2.0 Connection Capability profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-conn-capability-profile on page 4157 .
h2qp-op-cl-profile <profile-name>	Name of the Hotspot 2.0 Operating Class Indication profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-op-cl-profile on page 4159 .
h2qp-operator-friendly-name-profile <profile-name>	Name of the Hotspot 2.0 operator-friendly name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-operator-friendly-name-profile on page 4161 .
h2qp-osu-prov-list-profile <profile-name>	Name of the Hotspot 2.0 OSU providers list profile to be associated with this WLAN advertisement profile.
h2qp-wan-metrics-profile <profile-name>	Name of the Hotspot 2.0 WAN Metrics profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-wan-metrics-profile on page 4167 .
no	Negate or remove any existing parameter, returning it to its default value.
osu-ssid	NAme of the OSU SSID..

Example

The following example associates the ANQP domain name profile **anqp-dom-1** to the advertisement profile **network1**:

```
(host) [mynode] (config) #wlan hotspot advertisement-profile network1
```

```
(host) [mynode] (Advertisement Profile "network1") #anqp-domain-name-profile  
anqp-dom-1
```

Related Commands

Command	Description
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3rd Generation Partnership Project (3GPP) Cellular Network for hotspots that have roaming relationships with cellular operators
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot anqp-nai-realm-profile	This command defines a Network Access Identifier (NAI) realm whose information can be sent as an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response
wlan hotspot anqp-nwk-auth-profile	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.
wlan hotspot anqp-roam-cons-profile	This command configures the Roaming Consortium OI information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response
wlan hotspot anqp-venue-name-profile	This command defines venue information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot h2qp-conn-capability-profile	This command defines a Hotspot 2.0 Query Protocol (H2QP) profile that advertises hotspot protocol and port capabilities.
wlan hotspot h2qp-op-cl-profile	This command defines a Hotspot 2.0 Query Protocol (H2QP) profile that defines the Operating Class to be sent in the ANQP IE.

Command	Description
<u>wlan hotspot h2qp-operator-friendly-name-profile</u>	This command defines a Hotspot 2.0 Query Protocol (H2QP) operator-friendly name profile.
<u>wlan hotspot h2qp-wan-metrics-profile</u>	This command creates a Hotspot 2.0 Query Protocol (H2QP) profile that specifies the hotspot WAN status and link metrics.
<u>wlan hotspot hs2-profile</u>	This command configures a hotspot profile for an 802.11u public access service provider.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-3gpp-nwk-profile

```
wlan hotspot anqp-3gpp-nwk-profile <profile-name>  
  3gpp_plmn1 <3GPP-PLMN1>  
  3gpp_plmn2 <3GPP-PLMN2>  
  3gpp_plmn3 <3GPP-PLMN3>  
  3gpp_plmn4 <3GPP-PLMN4>  
  3gpp_plmn5 <3GPP-PLMN5>  
  3gpp_plmn6 <3GPP-PLMN6>  
  clone <source>  
no
```

Description

This command defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.

The 3GPP Cellular Network Profile defines an ANQP information element (IE) to be sent in a Generic Advertisement Service (GAS) query response from an AP in a hotspot with a roaming relationship with a cellular operator. The 3GPP Mobile Country Code (MCC) and the 12-bit Mobile Network Code data in the IE can help the client select a 3GPP network.

Values configured in this profile will not be sent to clients unless you:

Associate the 3GPP Cellular Network profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-3gpp-nwk-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. ("`wlan hotspot h2-profile advertisement-profile <profile-name>` ")

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
3gpp_plmn1	The Public Land Mobile Networks (PLMN) value of the highest-priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp_plmn2	The Public Land Mobile Networks (PLMN) value of the second-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp_plmn3	The Public Land Mobile Networks (PLMN) value of the third-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp_plmn4	The Public Land Mobile Networks (PLMN) value of the fourth-highest priority network.

Parameter	Description
	The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp_plmn5	The Public Land Mobile Networks (PLMN) value of the fifth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
3gpp_plmn6	The Public Land Mobile Networks (PLMN) value of the sixth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
clone <profile-name>	Copies an existing 3GPP profile.
no	Removes an existing parameter.

Example

The following example defines 3GPP data for the 3GPP profile **cellcorp1**:

```
(host) [md] (config) #wlan hotspot anqp-3gpp-nwk-profile cellcorp1
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #enable
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn1
310026
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn2
208000
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn3
208001
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-domain-name-profile

```
wlan hotspot anqp-domain-name-profile <profile-name>
  clone <source>
  domain-name <domain-name>
no
```

Description

This command defines the domain name to be sent in an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an Access Point, the AP will return an ANQP Information Element with the domain name configured in this profile.

Values configured in this profile are not sent to clients unless you:

Associate the ANQP Domain Name profile with an ANQP advertisement profile (`wlan hotspot advertisement profile <profile-name> anqp-domain-name-profile <profile-name>`).

Associate the ANQP advertisement profile with a Hotspot profile (`wlan hotspot h2-profile advertisement-profile <profile-name>`).

Enable the hotspot feature within that Hotspot profile (`wlan hotspot h2-profile <profile-name> hotspot-enable`).

Parameter	Description
<profile-name>	ANQP domain name profile.
clone <source>	Copies an existing ANQP domain name profile.
domain-name <domain-name>	Domain name of the hotspot operator. This alphanumeric string must be 255 characters or less.
no	Removes an existing parameter.

Example

The following example defines a domain name for the ANQP domain name profile domain1:

```
(host) [md] (config) #wlan hotspot anqp-domain-name-profile domain1
(host) [md] (ANQP Domain Name Profile "domain1") #domain-name example.com
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-ip-addr-avail-profile

```
wlan hotspot anqp-ip-addr-avail-profile <profile-name>
  clone <profile-name>
  ipv4-addr-avail {availability-unknown|not-available|port-restricted|port-
  restricted-double-nated|port-restricted-single-nated|private-double-
  nated|private-single-nated|public}
  ipv6-addr-avail {available|availability-unknown|not-available}
no
```

Description

This command defines available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response. The IP Address Availability information configured using this command provides clients with information about the availability of IP address versions and types which could be allocated to those clients after they associate to the hotspot AP.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP IP Address Availability profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-ip-addr-avail-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of the ANQP IP address availability profile.
clone <source>	Copies an existing ANQP IP Address Availability profile.
ipv4-addr-avail	Indicates the availability of an IPv4 network.
availability-unknown	Network availability cannot be determined.
not-available	Network is not available.
port-restricted	Network has some ports restricted (for example, the network blocks port 110 to restrict POP mail).
port-restricted-double-nated	Network has some ports restricted and multiple routers performing network address translation.
port-restricted-single-nated	Network has some ports restricted and a single router performing network address translation.

Parameter	Description
private-double-nated	Network is a private network with multiple routers doing network address translation.
private-single-nated	Network is a private network a single router doing network address translation.
public	Network is a public network.
ipv6-addr-avail	Indicates the availability of an IPv6 network.
available	An IPv6 network is available.
availability-unknown	Network availability cannot be determined.
not-available	Network is not available.
no	Removes an existing parameter.

Example

The following example configures an AP using this profile to advertise a public IPv4 network:

```
(host) [md] (config) #wlan hotspot anqp-ip-addr-avail-profile default
(host) [md] (ANQP IP Address Availability Profile "default") #ipv4-addr-avail public
(host) [md] (ANQP IP Address Availability Profile "default") #ipv6-addr-avail not-available
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-nai-realm-profile

```
wlan hotspot anqp-nai-realm-profile <profile-name>
  clone <source>
  nai-home-realm
  nai-realm-auth-id-1|nai-realm-auth-id-2 {credential-type|expanded-eap|expanded-
  inner-eap|inner-auth-eap|non-eap-inner-auth|reserved|tunneled-eap-credential-
  type}
  nai-realm-auth-value-1|nai-realm-auth-value-2 {cred-cert|cred-hw-token|cred-
  nfc|cred-none|cred-rsvd|cred-sim|cred-soft-token|cred-user-pass|cred-usim|cred-
  vendor-spec|eap-crypto-card|eap-generic-token-card|eap-identity|eap-method-
  aka|eap-method-sim|eap-method-tls|eap-method-ttls|eap-notification|eap-one-time-
  password|eap-peap|eap-peap-mschapv2|non-eap-chap|non-eap-mschap|non-eap-
  mschapv2|non-eap-pap|non-eap-rsvd|reserved|tun-cred-anon|tun-cred-cert|tun-cred-
  hw-token|tun-cred-nfc|tun-cred-rsvd|tun-cred-sim|tun-cred-soft-token|tun-cred-
  user-pass|tun-cred-usim|tun-cred-vendor-spec}
  nai-realm-eap-method crypto-card|eap-aka|eap-sim|eap-tls|eap-ttls|generic-token-
  card|identity|notification|one-time-password|peap|peap-mschapv2
  nai-realm-encoding <nai-realm-encoding>
  nai-realm-name <nai-realm-name>
  no
```

Description

This command defines a Network Access Identifier (NAI) realm whose information can be sent as an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

An AP's NAI Realm profile identifies and describes a NAI realm accessible using the AP, and the method that this NAI realm uses for authentication. These settings configured in this profile determine the NAI realm elements that are included as part of a GAS Response frame.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP NAI Realm profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name>anqp-nai-realm-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profileadvertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Parameter	Description
<profile-name>	Name of the ANQP NAI realm profile.
clone <source>	Copies an existing NAI Realm profile.

Parameter	Description
nai-home-realm	Marks the realm in this profile as the NAI Home Realm.
nai-realm-auth-id-1 nai-realm-auth-id-2	Use the <code>nai-realm-auth-id-1</code> command to send the one of the following authentication methods for the primary NAI realm ID. Use the <code>nai-realm-auth-id-2</code> command to send the one of the following authentication methods for the secondary NAI realm ID.
credential-type	The specified authentication ID uses credential authentication.
expanded-eap	The specified authentication ID uses the expanded EAP authentication method.
expanded-inner-eap	The specified authentication ID uses the expanded inner EAP authentication method.
inner-auth-eap	The specified authentication ID uses inner EAP authentication type.
non-eap-inner-auth	The specified authentication ID uses non-EAP inner authentication type.
reserved	The specified authentication ID uses Reserved authentication type.
tunneled-eap-credential-type	The specified authentication ID uses the tunneled EAP credential type.
nai-realm-auth-value-1 nai-realm-auth-value-2	Use the <code>nai-realm-auth-value-1</code> command to select an authentication value for the authentication method specified by nai-realm-auth-id-1 . Use the <code>nai-realm-auth-value-2</code> command to select the authentication value for the authentication method specified by nai-realm-auth-id-2 .
cred-cert	Credential - Certificate.
cred-hw-token	Credential - Hardware Token.
cred-nfc	Credential - NFC.
cred-none	Credential - None.
cred-rsvd	Credential - Reserved.

Parameter	Description
cred-sim	Credential - SIM.
cred-soft-token	Credential - Soft Token.
cred-user-pass	Credential - Username and password.
cred-usim	Credential - USIM.
cred-vendor-spec	Credential - Vendor-specific.
eap-crypto-card	EAP Method - Crypto-card.
eap-generic-token-card	EAP Method - Generic-Token-Card.
eap-identity	EAP Method - Identity.
eap-method-aka	EAP Method - AKA.
eap-method-sim	EAP Method - SIM - GSM Subscriber Iden.
eap-method-tls	EAP Method - TLS - Transport Layer Sec.
eap-method-ttls	EAP Method - TTLS - Tunneled Transport Security.
eap-notification	EAP Method - Notification.
eap-one-time-password	EAP Method - One-Time-Password.
eap-peap	EAP Method - PEAP.
eap-peap-mschapv2	EAP Method - PEAP MSCHAP V2.
non-eap-chap	Non-EAP Method - CHAP.
non-eap-mschap	Non-EAP Method - MSCHAP.
non-eap-mschapv2	Non-EAP Method - MSCHAPv2.
non-eap-pap	Non-EAP Method - PAP.
non-eap-rsvd	Non-EAP Method - Reserved for future use.
reserved	Reserved for future use.
tun-cred-anon	Tunneled Credential - ANONYMOUS.
tun-cred-cert	Tunneled Credential - CERTIFICATE .
tun-cred-hw-token	Tunneled Credential - Hardware Token.

Parameter	Description
tun-cred-nfc	Tunneled Credential - NFC.
tun-cred-rsvd	Tunneled Credential - RESERVED.
tun-cred-sim	Tunneled Credential - SIM.
tun-cred-soft-token	Tunneled Credential - Soft Token.
tun-cred-user-pass	Tunneled Credential - USERNAME and PASSWORD.
tun-cred-usim	Tunneled Credential - USIM.
tun-cred-vendor-spec	Tunneled Credential - VENDOR SPECIFIC.
nai-realm-eap-method	Select one of the options below to identify the EAP authentication method supported by the hotspot realm.
crypto-card	Crypto card authentication.
eap-aka	EAP for UMTS Authentication and Key Agreement.
eap-sim	EAP for GSM Subscriber Identity Modules.
eap-tls	EAP-Transport Layer Security.
eap-ttls	EAP-Tunneled Transport Layer Security.
generic-token-card	EAP Generic Token Card (EAP-GTC)
identity	EAP Identity type.
notification	The hotspot realm uses EAP Notification messages for authentication.
one-time-password	Authentication with a single-use password.
peap	Protected Extensible Authentication Protocol.
peap-mschapv2	Protected Extensible Authentication Protocol with Microsoft CHAP version 2.
nai-realm-encoding <nai-realm-encoding>	Issue this command if the NAI realm named defined by nai-realm-name <nai-realm-name> is a UTF-8 formatted character string that is not formatted in accordance with IETF RFC 4282.
nai-realm-name <nai-realm-name>	Name of the NAI realm. The realm name is often the domain name of the service provider.
no	Negates or removes any existing parameter

Example

The following example configures a Network Access Identifier (NAI) realm profile:

```
(host) [md] (config) #wlan hotspot anqp-nai-realm-profile home
(host) [md] (ANQP NAI Realm Profile "home") #enable
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-name corp-hotspot.com
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-auth-id-1 credential-
type
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-auth-value-1 cred-
cert
(host) [md] (ANQP NAI Realm Profile "home") #nai-home-realm
(host) [md] (config) #wlan hotspot anqp-nai-realm-profile non-home
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-name corp-
hotspot-roam.com
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-eap-method eap-
sim
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-auth credential-
type
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-nwk-auth-profile

```
wlan hotspot anqp-nwk-auth-profile <profile-name>
  clone <source>
  no
  nwk-auth-type {acceptance|dns-redirection|http-https-redirection|online-enroll}
  url <url>
```

Description

This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.

When you enable the [asra](#) option in the WLAN hotspot profile, the settings you configure in the Network Authentication profile are sent in the GAS response to the client.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP Network Authentication profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-nwk-auth-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of the ANQP network authentication profile.
clone <source>	Copies an existing ANQP Network Authentication profile.
no	Negates any existing parameter.
nwk-auth-type	Network authentication type being used by the hotspot network.
acceptance	Network requires the user to accept terms and conditions. NOTE: This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
dns-redirection	Additional information on the network is provided through DNS redirection. NOTE: This option requires you to specify a redirection URL string as an IP address, FQDN or URL.

Parameter	Description
http-https-redirect	Additional information on the network is provided through HTTP or HTTPS redirection.
online-enroll	Network supports online enrollment.
url <url>	URL, IP address, or FQDN used by the hotspot network for the acceptance or dns-redirect network authentication types.

Example

The following example configures the default Network Authorization profile to use DNS redirection:

```
(host) [md] (config) #wlan hotspot anqp-nwk-auth-profile default
(host) [md] (ANQP Network Authentication Profile "default") #nwk-auth-type
dns-redirect redirect-url http://www.example.com/redirect.html
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-roam-cons-profile

```
wlan hotspot anqp-roam-cons-profile <profile-name>  
  clone <source>  
  no  
  roam-cons oi <oi>
```

Description

This command configures the Roaming Consortium OI information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority. The Roaming Consortium IEs contain information identifying the network and service provider, whose security credentials can then be used to authenticate with the AP transmitting this element.

Use the [wlan hotspot anqp-roam-cons-profile](#) command to define the OI for the hotspot service provider in the ANQP Roaming Consortium profile. Values configured in this profile will not be sent to clients unless you:

Associate the ANQP Roaming Consortium profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-roam-cons-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)



NOTE

To identify additional Roaming consortium OIs used by the service provider's top three roaming partners, configure the [wlan hotspot hs2-profile](#), [wlan hotspot hs2-profile](#) or [wlan hotspot hs2-profile](#) parameters in the Hotspot Profile.

Parameter	Description
<profile-name>	Name of the ANQP roaming consortium profile.
clone <source>	Copies an existing ANQP Roaming Consortium profile.
no	Negates any existing parameter.
roam-cons oi <oi>	Sends the specified roaming consortium OI in a GAS query response. The OI must be a hexadecimal value.

Example

The following example defines the roaming consortium OI and OI length in the ANQP roaming consortium profile:

```
(host) [md] (config) #wlan hotspot anqp-roam-cons-profile profile1
(host) [md] (ANQP Roaming Consortium Profile "profile1") #roam-cons oi
506F9A
(host) [md] (ANQP Roaming Consortium Profile "profile1") #roam-cons-oi-len 3
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot anqp-venue-name-profile

```
wlan hotspot anqp-venue-name-profile <profile-name>
  clone
  no
  venue-group {outdoor|reserved|utility-
misc|vehicular|assembly|business|educational|factory-or-
industrial|institutional|mercantile|residential|storage|unspecified|utility-
misc|vehicular}
  venue-lang-code <venue-lang-code>
  venue-name <venue-name>
  venue-name-hex <venue-name-hex>
  venue-type <venue-type>
  venue-url <venue-url>
```

Description

This command defines venue information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Use this command to configure the venue group and venue type in an ANQP Venue Name profile. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an Access Point, the AP will return ANQP Information Elements with the values configured in this profile.

Values configured in this profile will not be sent to clients unless you:

Associate the ANQP Venue Name profile with an ANQP Advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-venue-name-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of the ANQP venue profile.
clone <source>	Copies an existing ANQP Venue Name profile.
no	Negates any existing parameter.
venue-group	Specify one of the following venue groups to be advertised in the ANQP IEs from APs associated with this profile. The default setting is unspecified. <ul style="list-style-type: none">■ assembly■ business■ educational■ factory-or-industrial■ institutional■ mercantile

Parameter	Description
	<ul style="list-style-type: none"> ■ outdoor ■ reserved ■ residential ■ storage ■ unspecified ■ utility-misc ■ vehicular
venue-lang-code <venue-lang-code>	An ISO 639 language code that identifies the language used in the Venue Name field.
venue-name <venue-name>	Venue name to be advertised in the ANQP IEs from APs associated with this profile. If the venue name includes spaces, the name must be enclosed in quotation marks, e.g. "Midtown Shopping Center".
venue-name-hex <venue-name-hex>	Venue name, in hex format, to be advertised in the ANQP IEs from APs associated with this profile.
venue-type <venue-type>	Specify a venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 4155 .
venue-url <venue-url>	Venue URL where customer may go to get additional information related to the venue.

Venue Types

The following list describes the different venue types that may be configured in a hotspot profile:

<ul style="list-style-type: none"> ■ assembly-amphitheater ■ assembly-amusement-park ■ assembly-arena ■ assembly-bar ■ assembly-coffee-shop ■ assembly-convention-center ■ assembly-emer-coord-center ■ assembly-library ■ assembly-museum ■ assembly-passenger-terminal ■ assembly-restaurant 	<ul style="list-style-type: none"> ■ business-police-station ■ business-post-office ■ business-professional-office ■ business-research-and-development ■ business-unspecified ■ educational-primary-school ■ educational-secondary-school ■ educational-university ■ educational-unspecified ■ industrial-factory ■ institutional-alcohol-or-drug-rehab ■ institutional-group-home 	<ul style="list-style-type: none"> ■ merchantile unspecified ■ outdoor-bus-stop ■ outdoor-city-park ■ outdoor-kiosk ■ outdoor-muni-mesh-nwk ■ outdoor-rest-area ■ outdoor-traffic-control ■ outdoor-unspecified ■ residential-boarding-house ■ residential-dormitory ■ residential-hotel ■ residential-private-residence
---	--	--

<ul style="list-style-type: none"> ■ assembly-stadium ■ assembly-theater ■ assembly-unspecified ■ assembly-worship-place ■ assembly-zoo ■ business-attorney ■ business-bank ■ business-doctor ■ business-fire-station 	<ul style="list-style-type: none"> ■ institutional-hospital ■ institutional-prison ■ institutional-terminal-care ■ institutional-unspecified ■ mercantile-automotive-service-station ■ mercantile-gas-station ■ mercantile-grocery ■ mercantile-retail ■ mercantile-shopping-mall 	<ul style="list-style-type: none"> ■ residential-unspecified ■ unspecified ■ vehicular-airplane ■ vehicular-automobile ■ vehicular-bus ■ vehicular-ferry ■ vehicular-motor-bike ■ vehicular-ship ■ vehicular-train ■ vehicular-unspecified
--	--	--

Example

The following example defines an ANQP Venue Name profile for a shopping mall:

```
(host) [md] (config) #wlan hotspot anqp-venue-name-profile Mallprofile1
(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-group mercantile
(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-name Westgate Shopping Center

(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-type mercantile-shopping-mall
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot h2qp-conn-capability-profile

```
wlan hotspot h2qp-conn-capability-profile <profile-name>
  clone <source>
  esp
  icmp
  no
  tcp-ftp
  tcp-http
  tcp-pptp-vpn
  tcp-ssh
  tcp-tls-vpn
  tcp-voip
  udp-ike2-4500
  udp-ike2-500
  udp-voip
```

Description

This command defines an H2QP profile that advertises hotspot protocol and port capabilities. The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about the IP protocols and associated port numbers that are available and open for communication.

Values configured in this profile will not be sent to clients unless you:

Associate the H2QP profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> h2qp-conn-cap-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of the H2QP connection capability profile.
clone <source>	Copies an existing hotspot connection capability profile.
esp	Include this parameter to enable the Encapsulating Security Payload (ESP) port used by IPsec VPNs. (port 0)
icmp	Indicates that the ICMP port is enabled and available. (port 0)
no	Negates any existing parameter, returning it to its default disabled value.
tcp-ftp	Include this parameter to enable the FTP port. (port 20)

Parameter	Description
tcp-http	Include this parameter to enable the HTTP port. (port 80)
tcp-pptp-vpn	Include this parameter to enable the PPTP port used by IPsec VPNs. (port 1723)
tcp-ssh	Include this parameter to enable the SSH port. (port 22)
tcp-tls-vpn	Include this parameter to enable the TCP TLS port used by VPNs. (port 80)
tcp-voip	Include this parameter to enable the TCP VoIP port. (port 5060)
udp-ike2-4500	Include this parameter to enable the IKEv2. (port 4500)
udp-ike2-500	Include this parameter to enable the IKEv2. (port 500)
udp-voip	Include this parameter to enable the UDP VoIP port. (port 5060)

Example

The following example allows the H2QP connection capability profile to advertise the availability of ICMP, HTTP, and VOIP ports:

```
(host) [md] (config) #wlan hotspot h2qp-conn-capability-profile Wan1
(host) [md] (H2QP Connection Capability Profile "Wan1") #icmp
(host) [md] (H2QP Connection Capability Profile "Wan1") #http
(host) [md] (H2QP Connection Capability Profile "Wan1") # voip
(host) [md] (H2QP Connection Capability Profile "Wan1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot h2qp-op-cl-profile

```
wlan hotspot h2qp-op-cl-profile <profile-name>
  clone <source>
  no
  op-cl <op-cl>
```

Description

This command defines an H2QP profile that defines the Operating Class to be sent in the ANQP IE.

The values configured in this H2QP Operating Class profile define the channels on which the hotspot is capable of operating. It may be useful where, for instance, a mobile device discovers a hotspot in the 2.4 GHz band but finds it is dual-band and prefers the 5 GHz band. For a definition of these global operating classes, refer to Table E-4 of IEEE Std 802.11-2012, Annex E.

Values configured in this profile will not be sent to clients unless you:

Associate the H2QP profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> h2qp-op-cl-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Parameter	Description
<profile-name>	Name of the H2QP operating class indication profile.
clone <source>	Copies an existing hotspot operating class profile.
no	Negates any existing parameter, returning it to its default disabled value.
op-cl <op-cl>	Configures the operating class for the devices' BSS. 1-255 1

Example

The following example configures and enables a profile with the default operating class value:

```
(host) [md] (config) #wlan hotspot h2qp-op-cl-profile profile1
(host) [md] (H2QP Operating Class Indication Profile "profile1") #op-cl 1
(host) [md] (H2QP Operating Class Indication Profile "profile1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot h2qp-operator-friendly-name-profile

```
wlan hotspot h2qp-operator-friendly-name-profile <profile-name>
  clone <source>
  no
  op-fr-name <op-fr-name>
  op-fr-name-hex <op-fr-name-hex>
  op-lang-code <op-lang-code>
```

Description

This command defines an H2QP operator-friendly name profile.

The operator-friendly name configured in this profile is a free-form text field that can identify the operator and also something about the location.

Values configured in this profile will not be sent to clients unless you:

Associate the H2QP operator-friendly name profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name>h2qp-operator-friendly-profile <profile-name>`)

Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)

Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Parameter	Description
<profile-name>	H2QP operator friendly name profile.
clone <source>	Copies an existing operator-friendly name profile.
no	Negates any existing parameter.
op-fr-name <op-fr-name>	An operator-friendly name sent by devices using this profile. The name can be up to 64 alphanumeric characters, and can include special characters and spaces. If the name includes quotation marks ("), you must include a backslash character (\) before each quotation mark. (e.g. \"example\")
op-fr-name-hex <op-fr-name-hex>	Operator Friendly Name in HEX.
op-lang-code <op-lang-code>	An ISO 639 language code that identifies the language used in the op-fr-name field.

Example

The following example shows that the managed device has two configured operator friendly name profiles. The **References** column lists the number of other profiles with references to the

operator friendly name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [md] (config) #wlan hotspot h2qp-operator-friendly-name-profile
profile1
(host) [md] (H2QP Operator Friendly Name Profile "profile1") #op-fr-name my_
hotspot
(host) [md] (H2QP Operator Friendly Name Profile "profile1") #op-lang-code
<op-lang-code>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

```
wlan hotspot h2qp-osu-prov-list-profile <profile>
  disable
  enable
  frnd-name-count <count>
  frnd-name1 <OSU Friendly name>
  frnd-name1-hex <OSU Friendly name>
  frnd-name1-lang-code <lang code>
  frnd-name2 <OSU Friendly name>
  frnd-name2-hex <OSU Friendly name>
  frnd-name2-lang-code <lang code>
  icon1-file <idx> <File Name>
  icon1-height <height>
  icon1-lang-code <lang code>
  icon1-type <file type>
  icon1-width <width>
  icon2-file <idx> <File Name>
  icon2-height <height>
  icon2-lang-code <lang code>
  icon2-type <file type>
  icon2-width <width>
  iconfile-count <count>
  no
  osu-method <OSU method>
  osu-server-uri <OSU server URI>
  srvc-desc1 <description>
  srvc-desc1-hex <description>
  srvc-desc1-lang-code <lang code>
  srvc-desc2 <description>
  srvc-desc2-hex <description>
  srvc-desc2-lang-code <lang code>
  srvcdesc-count <count>
```

Description

This command configures a H2QP profile that defines the Open Sign-Up(OSU) provider details to be sent in the H2QP IE.

Parameter	Description
disable	Disables the OSU provider profile.
enable	Enables the OSU provider profile. enabled
frnd-name-count	Number of OSU friendly names to be configured. 1-2

Parameter	Description
<code>frnd-name1</code>	The first OSU friendly name if you selected the language code as English. A string value of maximum 64 characters.
<code>frnd-name1-hex</code>	The first OSU friendly name in hexadecimal format for language codes other than English.
<code>frnd-name1-lang-code</code>	The language code used for configuring the first OSU friendly name.
<code>frnd-name2</code>	The second OSU friendly name if the language code chosen is English. A string value of maximum 64 characters.
<code>frnd-name2-hex</code>	The second OSU friendly name in hexadecimal format for language codes other than English.
<code>frnd-name2-lang-code</code>	The language code used for configuring the second OSU friendly name.
<code>icon1-file</code>	The index and name of the first icon image file.
<code>icon1-height</code>	Height of the first icon image file.
<code>icon1-lang-code</code>	Indicates the language used in the first icon image.
<code>icon1-type</code>	Type of the image file used as first icon.
<code>icon1-width</code>	Width of the first icon image file. 1-256
<code>icon2-file</code>	The index and name of the second icon image file.
<code>icon2-height</code>	Height of the second icon image file.
<code>icon2-lang-code</code>	Indicates the language used in the second icon image.
<code>icon2-type</code>	Type of the image file used as second icon.
<code>icon2-width</code>	Width of the second icon image file.
<code>iconfile-count</code>	Number of icon files to be used for the OSU provider. 1-2
<code>no</code>	Deletes the command.
<code>osu-method</code>	Indicates the method used by OSU to provision the HS2 client. OMA-DM, SOAP-XML
<code>osu-server-uri</code>	The URI of the OSU Server that is used for OSU with the service provider configured in the <code>frnd-name1</code> parameter.

Parameter	Description
srvc-desc1	The first service description if you selected the language code as English.
srvc-desc1-hex	The first service description in hexadecimal format for language codes other than English.
srvc-desc1-lang-code	The language code used for the first description.
srvc-desc2	The second service description if you selected the language code as English.
srvc-desc2-hex	The second service description in hexadecimal format for language codes other than English.
srvc-desc2-lang-code	The second service description if you selected the language code as English.
srvcdesc-count	Number of descriptions to be provided for the OSU provider.

Example

The following example creates and configures an OSU provider profile:.

```
(host) (config) # hotspot h2qp-osu-provider-profile OSU
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name-count 2
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name1-lang-code
"eng"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name1 "SP Red
Test Only"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name1-hex
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name2-lang-code
"kor"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name2 ""
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # frnd-name2-hex
535020ebb9a8eab09520ed858cec8aa4ed8ab820eca084ec9aa9
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # iconfile-count 2
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon1-width 128
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon1-height 61
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon1-lang-code zxx
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon1-type image/png
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon1-file 1 "icon_
red_zxx.png"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon2-width 160
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon2-height 76
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon2-lang-code eng
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon2-type image/png
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # icon2-file 2 "icon_
red_eng.png"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # srvcdesc-count 2
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # srvc-desc1-lang-code
eng
```

```
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # svc-desc1 "Free
service for test purpose"
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # svc-desc1-hex
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # svc-desc2-lang-code
kor
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # svc-desc2 ""
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # svc-desc2-hex
ed858cec8aa4ed8ab820ebaaa9eca081ec9cbceba19c20ebacb4eba38c20ec849cebb984ec8a
a4
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # osu-server-uri
https://osu-server.r2-testbed-ar.wi-
fi.org:443/guest/HotSpot2OnlineSignUp.php
(host) [mynode] (H2QP OSU Providers List Profile "OSU") # osu-method SOAP-XML
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan hotspot h2qp-wan-metrics-profile

```
wlan hotspot h2qp-wan-metrics-profile <profile-name>
  at-capacity
  clone <source>
  downlink-load
  downlink-speed
  load-dur
  no
  symm-link
  uplink-load
  uplink-speed
  wan-metrics-link-status link_down|link_test|link_up|reserved
```

Description

This command creates an H2QP profile that specifies the hotspot WAN status and link metrics. The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about access network characteristics such as link status and the capacity and speed of the WAN link to the Internet. Issue this command without the `<profile-name>` parameter to display the entire WAN metrics profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Parameter	Description
<code><profile-name></code>	Name of the H2QP WAN metrics profile.
<code>at_capacity</code>	Use the <code>at_capacity</code> parameter to indicate that the WAN Link has reached its maximum capacity. If this parameter is enabled, no additional mobile devices will be permitted to associate with the hotspot AP. enabled, disabled disabled
<code>clone <source></code>	Copies an existing H2QP profile.
<code>downlink-load <load></code>	The percentage of the WAN downlink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified. 1-100 0 (unspecified)

Parameter	Description
downlink-speed <speed>	Use the <code>downlink_speed <speed></code> parameter to indicate the current WAN backhaul downlink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified. 0 - 2,147,483,647 Kbps 0 (unspecified)
load-dur <load_dur>	Duration over which the downlink load is measured, in tenths of a second. 0 and 65535
no	Negates any existing parameter
symm-link	Use the <code>symn_link</code> parameter to indicate that the WAN Link has same speed in both the uplink and downlink directions. enabled, disabled disabled
uplink-load <speed>	The percentage of the WAN uplink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified. 1-100 0 (unspecified)
uplink-speed <speed>	Use the <code>uplink <speed></code> parameter to indicate the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified. 0 - 2,147,483,647 Kbps 0 (unspecified)
wan-metrics-link-status	Define the status of the WAN Link by configuring one of the following values. The default link status is reserved , which indicates that the link status is unknown or unspecified. link_down, link_test, link_up, reserved reserved
link_down	WAN link is down.
link_test	WAN link is currently in a test state.
link_up	WAN link is up.
reserved	This parameter is reserved by the Hotspot 2.0 specification, and cannot be configured. This is the default link status.

Example

The following example shows three WAN metrics profiles that are configured. The **References** column lists the number of other profiles with references to the operator-friendly name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [md] #show wlan hotspot h2qp-wan-metrics-profile
H2QP WAN Metrics Profile List
-----
Name           References  Profile Status
----           -
default        0
WanFastlink

Total:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan hotspot hs2-profile

```
wlan hotspot hs2-profile <profile-name>
  access-network-type {emergency-services|personal-device|private|private-
  guest|public-chargeable|public-free|test|wildcard}
  advertisement-profile <profile-name>
  advertisement-protocol {anqp|eas|mih-cmd-event|mih-info|rsvd}
  anqp-domain-id
  asra
  clone <source>
  comeback-mode
  dscp-exceptions
  dscp-ranges
  gas-comeback-delay <gas-comeback-delay>
  grp-frame-block
  hessid <hessid>
  hotspot-enable
  hotspot-osen
  hotspot-roam-cons-oi-1
  hotspot-roam-cons-oi-2
  hotspot-roam-cons-oi-3
  internet
  no
  osu-nai
  p2p-cross-connect
  p2p-dev-mgmt
  pame-bi
  query-response-length-limit <query-response-length-limit>
  radius-cui
  radius-loc-data
  reauth-delay
  release-number {release-1|release-2|reserved}
  session-info-url
  sub-deauth-reason-url
  sub-rem-server-url
  time-advt-cap {no-std-ext-timesrc|timestamp-offset-utc|reserved}
  time-error <milliseconds>
  time-zone <time-zone>
  venue-group <venue-group>
  venue-type <venue-type>
```

Description

This command configures a hotspot profile for an 802.11u public access service provider.

Hotspot 2.0 is a WFA specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

Mobility Conductor supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue and type via management frames from the Aruba AP. Clients can also query APs for information about the network's

available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

Parameter	Description
<profile-name>	Name of the hotspot profile.
access-network-type	Specifies the 802.11u network type. The default setting is public-chargeable . <ul style="list-style-type: none"> ■ emergency-services: emergency services only network ■ personal-device: personal device network ■ private: private network ■ private-guest: private network with guest access ■ public-chargeable: public chargeable network ■ public-free: free public network ■ test: test network ■ wildcard: wildcard network
advertisement-profile <profile-name>	Advertisement profile associated with this hotspot profile. If this parameter is not changed, the hotspot profile uses with the default advertisement profile.
advertisement-protocol	Select one of the following advertisement protocol types to be used by the AP. <ul style="list-style-type: none"> ■ anqp ■ emergency: Emergency Alert System ■ mih-cmd-event: Media Independent Handover Command and Event Services Capability Discovery ■ mih-info: Media Independent Handover Information Service. This option allows handovers between differing kinds of wireless access protocols and technologies, allowing access points on different IP subnets to communicate with each other at the link level while maintaining session continuity. ■ rsvd: Reserved for future use.
anqp-domain-id <anqp-domain-id>	Number representing the ANQP Domain ID. Zero means no domain.
asra	Issue the Additional Steps Required for Access (ASRA) sub command if any additional steps are required for network access. If this parameter is enabled, the AP will send the following IEs in response to the client's ANQP query. <ul style="list-style-type: none"> ■ Venue Name ■ Domain Name List ■ Network Authentication Type ■ Roaming Consortium List ■ NAI Realm List <p>NOTE: If ASRA is enabled, the advertisement profile for this hotspot must reference an enabled network</p>

Parameter	Description
	authentication type profile. For more information on enabling an network authentication type profile, see wlan hotspot anqp-nwk-auth-profile on page 4150 .
clone <source>	Makes a copy of an existing hotspot profile.
comeback-mode	By default, ANQP information is obtained from a GAS Request and Response. If you enable the comeback-mode option, advertisement information is obtained using a GAS Request and Response, as well as a Comeback-Request and Comeback-Response. This option is disabled by default.
dscp-exceptions <dscp-exceptions>	QoS Map DSCP Exception fields. These can be upto 21 sets <value>:<up> separated by ',' where value is 0-3F or FF, and up is 0-7) Format Example: DSCP:UP[,DSCP:UP]
dscp-ranges	QoS Map DSCP Ranges. There are total 8 sets <low>:<high> separated by ',' where low and high are 0-3F or FF. Example: 08-0F,00-07,FF-FF,10-1F,20-27,FF-FF,28-2F,30-3F
gas-comeback-delay <gas-comeback-delay>	At the end of the GAS comeback delay interval, the client may attempt to retrieve the query response using a Comeback Request Action frame. The supported range is 100-2000 milliseconds, and the default value is 500 milliseconds.
grp-frame-block	This option configures the Downstream Group Addressed Forwarding Disabled Mode. If this feature is enabled, it ensures that the AP does not forward downstream group-addressed frames. It is disabled by default, allowing the AP to forward downstream group-addressed frames.
hessid <hessid>	This optional parameter devices an AP's homogenous ESS identifier, which is that device's MAC address in colon-separated hexadecimal format.
hotspot-enable	Enables or disables the hotspot. When this feature is enabled, the Information Elements (IEs) for this hotspot are included in beacons and probe responses from the AP. This setting is disabled by default.
hotspot-osen	Enables or disables the hotspot osen.
hotspot-roam-cons-oi-1	Roaming Consortium entry 1 OI value and length.
hotspot-roam-cons-oi-2	Roaming Consortium entry 2 OI value and length.

Parameter	Description
hotspot-roam-cons-oi-3	Roaming Consortium entry 3 OI value and length.
internet	If you issue the <code>internet</code> parameter, the AP sends an IE indicating that the network allows internet access. By default, a hotspot profile does not advertise network internet access.
no	Negates or removes any configured parameter.
osu-nai	OSU NAI for OSEN.
p2p-cross-connect	Issue this command to advertise support for P2P Cross Connections. This setting is disabled by default.
p2p-dev-mgmt	Issue this command to advertise support for P2P device management. This setting is disabled by default.
pame-bi	This option enables the Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, which is used by an AP to indicate whether the AP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.
query-response-length-limit <query-response-length-limit>	GAS enables advertisement services that lets clients query multiple 802.11 networks at once, while also allowing the client to learn more about a network's 802.11 infrastructure before associating. If a client transmits a GAS Query using a GAS Initial Request frame, the responding AP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame. This parameter sets the maximum length of the GAS query response, in octets. The supported range is 1-255 octets.
radius-cui	Include this parameter to enable the Chargeable-User-Identity RADIUS attribute defined by RFC 4372. Home networks can use this attribute to identify a user for the roaming transactions that take place outside of that home network.
radius-loc-data	Include this parameter to enable the Location Data RADIUS attribute defined by RFC 5580. Enabling this parameter allows the RADIUS server to use location data.
reauth-delay <reauth-delay>	Delay required before STA can re-auth with AP after it is deauthenticated.
release number	Hotspot 2.0 Release Number: <ul style="list-style-type: none"> ■ Release #1 ■ Release #2 ■ Reserved

Parameter	Description
session-info-url <session-info-url>	Specify URL for the Session Information Server.
sub-death-reason-url	Specify URL that explains why STA was not authorized or is no longer authorized.
sub-rem-server-url	Specify URL for the Subscription Remediation Server.
time-advt-cap no-std-ext-timesrc timestamp-offset-utc reserved	<p>This parameter specifies the AP's source of external time, and the current condition of its timing estimator.</p> <ul style="list-style-type: none"> ■ no-std-ext-time-src: The AP using this profile has no standardized external time source. ■ timestamp-offset-utc: The AP has a timestamp offset based on UTC. ■ reserved: This setting is reserved for future use, and should not be used.
time-error	The standard deviation of error in time value estimate, in milliseconds. The default value is 0 milliseconds, and the supported range is 0- 2,147,483,647 milliseconds.
time-zone	<p>The time zone in which the AP is operating, in the format <std><offset>[dst[offset] [,start[/time],end[/time]]]</p> <p>Where the <std> string specifies the abbreviation of the time zone, <dst> is the abbreviation of the timezone in daylight savings time, and the <offset> string specifies the time value you must add to the local time to arrive at UTC.</p> <p>NOTE: For complete details on configuring the timezone format, refer to section 8.3 of IEEE Std 1003.1, 2004 Edition.</p>
venue-group <venue-group>	<p>Specify one of the following venue groups to be advertised in the IEs from APs associated with this hotspot profile. The default setting is unspecified.</p> <ul style="list-style-type: none"> ■ assembly ■ business ■ educational ■ factory-or-industrial ■ institutional ■ mercantile ■ outdoor ■ reserved ■ residential ■ storage ■ unspecified ■ utility-misc ■ vehicular

Parameter	Description
	<p>NOTE: This parameter only defines the venue group advertised in the IEs from hotspot APs. To define the venue group to be included in ANQP responses, use anqp-venue-name-profile <profile-name>.</p>
venue-type <venue-type>	<p>Specify a venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 4176</p> <p>NOTE: This parameter only defines the venue type advertised in the IEs from hotspot APs. To define the venue type to be included in ANQP responses, use anqp-venue-name-profile <profile-name>.</p>

Generic Advertisement Service Queries

An Organization Identifier is a unique identifier assigned to a service provider when it registers with the IEEE registration authority. An AP can include its service provider OI in beacons and probe responses to clients. If a client recognizes an AP's OI, it will attempt to associate to that AP using the security credentials corresponding to that service provider.

If the client does *not* recognize the AP's OI, that client can send a GAS query to the AP to request more information more about the network before associating.

ANQP Information Elements

ANQP IEs are additional data that can be sent from the AP to the client to identify the AP's network and service provider. If a client requests this information via a GAS query, the hotspot AP then sends the ANQP Capability list in the GAS Initial Response frame indicating support for the following IEs:

- **Venue Name:** defined using the [wlan hotspot anqp-venue-name-profile](#) command.
- **Domain Name:** defined using the [wlan hotspot anqp-domain-name-profile](#) command.
- **Network Authentication Type:** defined using the [wlan hotspot anqp-nwk-auth-profile](#) command.
- **Roaming Consortium List:** defined using the [wlan hotspot anqp-roam-cons-profile](#) command.
- **AI Realm:** defined using the [wlan hotspot anqp-nai-realm-profile](#) command.
- **Cellular Network Data:** defined using the [wlan hotspot anqp-3gpp-nwk-profile](#) command.
- **Connection Capability:** defined using the [wlan hotspot h2qp-conn-capability-profile](#) command.
- **Operator Class:** defined using the [wlan hotspot h2qp-op-cl-profile](#) command.
- **Operator Friendly Name:** defined using the [wlan hotspot h2qp-operator-friendly-name-profile](#) command.
- **WAN Metrics:** defined using the [wlan hotspot h2qp-wan-metrics-profile](#).

Roaming Consortium OIs

Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority. You can specify the OI for the hotspot's service provider in the ANQP Roaming Consortium profile using the [wlan hotspot anqp-roam-cons-profile](#) command. This Hotspot profile also allows you to define and send up to three additional roaming consortium OIs for the service provider's top three roaming partners. To send this additional data to clients, you must specify the number of roaming consortium elements a client can query using the `add1-roam-cons-ois <1-3>` parameter, then define those elements using the following parameters:

- `roam-cons-oi-1` and `roam-cons-len 1`
- `roam-cons-oi-2` and `roam-cons-len 2`
- `roam-cons-oi-3` and `roam-cons-len 3`

The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Venue Types

The following list describes the different venue types that may be configured in a hotspot profile:

■ <code>assembly-amphitheatre</code>	■ <code>business-fire-station</code>	■ <code>mercantile-shopping-mall</code>
■ <code>assembly-amusement-park</code>	■ <code>business-police-station</code>	■ <code>outdoor-bus-stop</code>
■ <code>assembly-arena</code>	■ <code>business-post-office</code>	■ <code>outdoor-city-park</code>
■ <code>assembly-bar</code>	■ <code>business-professional-office</code>	■ <code>outdoor-kiosk</code>
■ <code>assembly-coffee-shop</code>	■ <code>business-research-and-development</code>	■ <code>outdoor-muni-mesh-nwk</code>
■ <code>assembly-convention-center</code>	■ <code>educational-primary-school</code>	■ <code>outdoor-rest-area</code>
■ <code>assembly-emer-coord-center</code>	■ <code>educational-secondary-school</code>	■ <code>outdoor-traffic-control</code>
■ <code>assembly-library</code>	■ <code>educational-university</code>	■ <code>residential-boarding-house</code>
■ <code>assembly-museum</code>	■ <code>industrial-factory</code>	■ <code>residential-dormitory</code>
■ <code>assembly-passenger-terminal</code>	■ <code>institutional-alcohol-or-drug-rehab</code>	■ <code>residential-hotel</code>
■ <code>assembly-restaurant</code>	■ <code>institutional-group-home</code>	■ <code>residential-private-residence</code>
■ <code>assembly-stadium</code>	■ <code>institutional-hospital</code>	■ <code>unspecified</code>
■ <code>assembly-theater</code>	■ <code>institutional-prison</code>	■ <code>vehicular-airplane</code>
■ <code>assembly-worship-place</code>	■ <code>institutional-terminal-care</code>	■ <code>vehicular-automobile</code>
■ <code>assembly-zoo</code>	■ <code>mercantile-automotive-service-station</code>	■ <code>vehicular-bus</code>
■ <code>business-attorney</code>	■ <code>mercantile-gas-station</code>	■ <code>vehicular-ferry</code>
■ <code>business-bank</code>	■ <code>mercantile-grocery</code>	■ <code>vehicular-motor-bike</code>
■ <code>business-doctor</code>	■ <code>mercantile-retail</code>	■ <code>vehicular-ship</code>
		■ <code>vehicular-train</code>

Example

The following example configures a hotspot profile with one additional roaming consortium OI for the service provider's top roaming partner:

```
(host) [md] (config) #wlan hotspot hs2-profile profile2
(host) [md] (Hotspot 2.0 Profile "profile2") #venue-group mercantile(host)
[md] (Hotspot 2.0 Profile "profile2") #venue-type mercantile-shopping-mall
(host) [md] (Hotspot 2.0 Profile "profile2") #addtl-roam-cons-ois
(host) [md] (Hotspot 2.0 Profile "profile2") #roam-cons-len 3
(host) [md] (Hotspot 2.0 Profile "profile2") #roam-cons-oil 415B8C
{host) [md] (Hotspot 2.0 Profile "profile2") #hotspot-enable
```

Related Commands

Command	Description
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an ANQP information element in a GAS query response.
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an ANQP information element in a GAS query response.
wlan hotspot anqp-nai-realm-profile	This command defines a Network Access Identifier realm whose information can be sent as an ANQP information element in a GAS query response
wlan hotspot anqp-nwk-auth-profile	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.
wlan hotspot anqp-roam-cons-profile	This command configures the Roaming Consortium OI information to be sent in an ANQP information element in a GAS query response
wlan hotspot anqp-venue-name-profile	This command defines venue information be sent in an ANQP information element in a GAS query response.
wlan hotspot h2qp-conn-capability-profile	Defines a H2QP profile that advertises hotspot protocol and port capabilities.

Command	Description
<u>wlan hotspot h2qp-op-cl-profile</u>	Defines a H2QP profile that defines the Operating Class to be sent in the ANQP IE.
<u>wlan hotspot h2qp-operator-friendly-name-profile</u>	Defines a H2QP operator-friendly name profile.
<u>wlan hotspot h2qp-wan-metrics-profile</u>	Creates a H2QP profile that specifies the hotspot WAN status and link metrics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan ht-ssid-profile

```
wlan ht-ssid-profile <profile-name>
  40MHz-enable
  80MHz-enable
  ba-amsdu-enable
  clone <profile-name>
  high-throughput-enable
  ldpc
  legacy-stations
  max-rx-a-mpdu-size {8191|16383|32767|65535}
  max-tx-a-mpdu-size <bytes>
  max-tx-a-msdu-count-be {0-15}
  max-tx-a-msdu-count-bk {0-15}
  max-tx-a-msdu-count-vi {0-15}
  max-tx-a-msdu-count-vo {0-15}
  max-vht-mpdu-size
  min-mpdu-start-spacing {0|.25|.5|1|2|4|8|16}
  mpdu-agg
  no...
  rx-ampdu
  short-guard-intvl-20MHz
  short-guard-intvl-40MHz
  short-guard-intvl-80MHz
  stbc-rx-streams
  stbc-tx-streams
  supported-mcs-set <mcs-list>
  temporal-diversity
  very-high-throughput-enable
  vht-mu-txbf-enable
  vht-supported-mcs-map
  vht-txbf-explicit-enable
  vht-txbf-sounding-interval
```

Description

This command configures a high-throughput SSID profile.

The ht-ssid profile configures the high-throughput SSID. Stations are not allowed to use HT with TKIP stand-alone encryption, although TKIP can be provided in mixed-mode BSSIDs that support HT. HT is disabled on a BSSID if the encryption mode is stand-alone TKIP or WEP.

You can also use this profile to configure explicit transmit beamforming for 130 Series access points. When this feature is enabled, the AP coordinates the signals sent from each antenna so the signals focus on the receiver, improving radio range and performance. The 130 Series AP can advertise transmit beamforming capabilities in beacon, probe response and association responses in the HT capabilities IE, then use the compressed or noncompressed beamforming report from clients to form a steering matrix. The AP ensures that the steering matrix stays current by updating and recalibrating the steering matrix at regular intervals.

By default, 130 Series access points support both compressed and non-compressed steering information from clients. If you have many clients that can send only non-compressed steering

reports, best practices are to retain the default settings, allowing the AP to support both types of steering reports. If all (or nearly all) of the AP's clients are capable of sending compressed steering reports, best practices are to disable non-compressed steering in the AP's HT SSID profile.

De-aggregation of MSDUs is supported with a maximum frame transmission size of 4 KBs; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

Parameter	Description
<profile-name>	Name of this instance of the profile. The name must be 1-63 characters. default
40MHz-enable	Enables or disables the use of this high-throughput SSID in 40 MHz mode. enabled
80MHz-enable	Enables or disables the use of 80 MHz channels on VHT APs. enabled
ba-amsdu-enable	Enables or disables Receive AMSDU in Block ACK (BA) negotiation. If disabled, AP denies clients from sending AMSDU using BA agreement. enabled
clone	Name of an existing high-throughput SSID profile from which parameter values are copied.
high-throughput-enable	Enables or disables high-throughput SSID to allow high-throughput (802.11n) stations to associate. Enabling high-throughput in an ht-ssid-profile enables WMM base features for the associated SSID. enabled
ldpc	If enabled, the AP will advertise LDPC support. LDPC improves data transmission over radio channels with high levels of background noise. enabled
legacy-stations	Controls whether or not legacy (non-HT) stations are allowed to associate with this SSID. By default, legacy stations are allowed to associate. This setting has no effect on a BSS in which HT support is not available. enabled
max-rx-a-mpdu-size	Controls the maximum size, in bytes, of an A-MPDU that can be received on this high-throughput SSID.

Parameter	Description
	8191, 16383, 32767, 65535 65535
8191	Maximum size of 8191 bytes.
16383	Maximum size of 16383 bytes.
32767	Maximum size of 32767 bytes.
65535	Maximum size of 65535 bytes.
max-tx-a-mpdu-size	Controls the maximum size, in bytes, of an A-MPDU that can be sent on this high-throughput SSID. 1576-65535 65535
max-tx-a-masdu-count-be	Sets the maximum number of MSDUs in a TX A-MSDU on best effort AC. NOTE: In tunnel and decrypt-tunnel forwarding mode, TX A-MSDU is disabled if the value is set to 0. If the value is set to non-zero, TX A-MSDU is enabled and set to this value. 0-15 2
max-tx-a-masdu-count-bk	Sets the maximum number of MSDUs in a TX A-MSDU on background AC. NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on background AC is disabled and assigning any value has no effect. 0-15 2
max-tx-a-masdu-count-vi	Sets the maximum number of MSDUs in a TX A-MSDU on video AC. NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on video AC is disabled and assigning any value has no effect. 0-15 2
max-tx-a-masdu-count-vo	Sets the maximum number of MSDUs in a TX A-MSDU on voice AC.

Parameter	Description
	<p>NOTE: TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on voice AC is disabled and assigning any value has no effect.</p> <p>0-15 0</p>
max-vht-mpdu-size	<p>Maximum size of a VHT MPDU. 3895, 7991, or 11454 bytes 11454 bytes</p>
min-mpdu-start-spacing	<p>Minimum time between the start of adjacent MDPUs within an aggregate MPDU in microseconds. 0, .25, .5, 1, 2,4, 8,16 0</p>
0	No restriction on MPDU start spacing.
.25	Minimum time of .25 μ sec.
.5	Minimum time of .5 μ sec.
1	Minimum time of 1 μ sec.
2	Minimum time of 2 μ sec.
4	Minimum time of 4 μ sec.
8	Minimum time of 8 μ sec.
16	Minimum time of 16 μ sec.
mpdu-agg	<p>Enables or disables MAC protocol data unit (MPDU) aggregation. High-throughput APs are able to send aggregated MDPUs, which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU. enabled</p>
no	Negates any configured parameter.
rx-ampdu	Enables or disables Receive AMPDU in Block ACK (BA) negotiation.

Parameter	Description
short-guard-intvl-20MHz	<p>Enables or disables use of short guard interval (400 ns) in 20 MHz mode.</p> <p>A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.</p> <p>enabled</p>
short-guard-intvl-40MHz	<p>Enables or disables use of short guard interval (400 ns) in 40 MHz mode of operation.</p> <p>enabled</p>
short-guard-intvl-80MHz	<p>Enables or disables use of short guard interval (400 ns) in 80 MHz mode of operation.</p> <p>enabled</p>
stbc-rx-streams	<p>Control the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.)</p> <p>NOTE: If transmit beamforming is enabled, STBC will be disabled for beamformed frames.</p> <p>0-1 1</p>
stbc-tx-streams	<p>Control the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.)</p> <p>NOTE: If transmit beamforming is enabled, STBC will be disabled for beamformed frames.</p> <p>0-1 1</p>

Parameter	Description
supported-mcs-set	<p>A list of MCS values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz vs. 80 MHz) and the number of spatial streams used by the mesh node.</p> <p>To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma.</p> <p>Examples: 2-10 1,3,6,9,12 MCS value of 16-23 are supported on 130 Series/RAP-155/11ac APs only. MCS value of 24-31 are supported on 320 Series APs only. 0-31</p>
temporal-diversity	<p>Enable or disable temporal diversity. When this setting is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries.</p> <p>disabled</p>
very-high-throughput-enable	<p>Enable or disable support for VHT (802.11ac) on the SSID.</p> <p>enabled</p>
vht-mu-txbf-enable	<p>Enable or disable VHT Multi-User Transmit Beamforming. If this parameter is disabled, all other Multi-User Transmit Beamforming configuration parameters have no effect.</p> <p>NOTE: This parameter is applicable for 320 Series APs only.</p> <p>enabled</p>
vht-supported-mcs-map	<p>Comma separated list of maximum supported MCS for spatial streams 1 through 4. Valid values for maximum MCS are 7, 8, 9, and '-' (if spatial stream is not supported). Maximum MCS of a spatial stream cannot be higher than the previous streams. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx.</p> <p>7, 8, 9, or - 9,9,9,9</p>
vht-txbf-explicit-enable	<p>Enable or disable VHT Explicit Transmit Beamforming for the 802.11ac-capable APs. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this parameter is disabled, all other transmit beamforming settings will not take effect.</p>

Parameter	Description
	enabled
vht-txbf-sounding-interval	<p>Time interval in milliseconds between channel information updates between the AP and the beamformee client.</p> <p>NOTE: This is applicable for 802.11ac-capable APs only.</p> <p>1-1000 msec 25 msec</p>

Example

The following example configures the maximum size of a received aggregate MPDU to be 8191 bytes for the high-throughput SSID named htcorpnet:

```
(host) [md] (config) #wlan ht-ssid-profile htcorpnet
(host) [md] (High-throughput SSID profile "htcorpnet") #max-rx-a-mpdu-size
8191
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
<p>All platforms, but only operates with 802.11n-capable APs. The following parameters are supported on 802.11ac-capable APs only:</p> <ul style="list-style-type: none"> ■ 80-MHz-enable ■ very-high-throughput-enable ■ vht-supported-mcs-map ■ vht-txbf-explicit-enable ■ vht-txbf-sounding-interval 	Base operating system	Config mode on Mobility Conductor.

wlan mu-edca-parameters-profile

```
wlan mu-edca-parameters-profile <profile-name>
  clone
  mu-background
  mu-best-effort
  mu-video
  mu-voice
  no
```

Description

This command configures an MU EDCA profile for APs or for clients (stations).

MU EDCA profiles are specific either to APs or clients. You apply an MU EDCA profile to a specific SSID profile. Use this command only under the guidance of your Aruba technical support representative.

Parameter	Description
<profile-name>	Name of the profile.
clone <source>	Copy data from another MU EDCA parameters profile.
no	Remove or negate a parameter.
mu-background	EDCA parameters for background queue.
mu-best-effort	EDCA parameters for best-effort queue.
mu-video	EDCA parameters for video queue.
mu-voice	EDCA parameters for voice queue.
aifsn <1-15>	Arbitrary inter-frame space number
ecw-max <0-15>	Maximum contention window (exponent)
ecw-min <0-15>	Minimum contention window (exponent)
timer <0-255>	MU EDCA Timer.

Example

The following example configures an EDCA profile for APs:

```
(host) [/md] (config) #wlan mu-edca-parameters-profile default
(host) [/md] (EDCA Parameters profile (AP) "default") #best-effort ecw-min
15 ecw-max 15 aifsn 15 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Conductor

wlan rrm-ie-profile

```
wlan rrm-ie-profile <profile-name>
  bss-aac-ie
  clone
  country-ie
  enabled-capabilities-ie
  no
  pwr-constraint-ie
  qbss-load-ie
  quiet-ie
  tpc-report-ie
```

Description

This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled. ArubaOS supports RRM IEs for APs with 802.11k support enabled. All IEs are sent by default.

Parameter	Description
bss-aac-ie	The AP will advertise in beacon and probe responses the BSS Available Admission Capacity IE, which contains information about the admission capabilities for each User Priority or AC.
clone	Copy the settings of an existing RRM IE profile.
country-ie	The AP will advertise in beacon and probe responses the device's regulatory domain.
enabled-capabilities-ie	The AP will advertise in beacon and probe responses support for radio measurements in a device.
no ...	Disables the transmission of an IE in this profile.
pwr-constraint-ie	The AP will advertise in beacon and probe responses the regulatory maximum transmit power for that current channel.
qbss-load-ie	The AP will advertise in beacon and probe responses the QBSS Load IE, which contains information on the current station count, channel utilization and available admission capacity levels in the QBSS.
quiet-ie	The AP will advertise in beacon and probe responses the Quiet IE, which is used to silence the channel for measurement purposes. When an AP uses a quiet IE to schedule a quiet interval, stations may not transmit on that channel during the quiet interval.
tpc-report-ie	The AP will advertise in beacon and probe responses information about its TCP.

Example

The following example prevents the AP from advertising the country IE:

```
(host) [md] (config) #wlan rrm-ie-profile default
(host) [md] (RRM IE Profile "default") #no country-ie
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Conductor.

wlan sae-profile

```
wlan sae-profile
  anti-clogging-token-threshold <anti-clogging-token-threshold>
  auth-frame-retransmit-interval <auth-frame-retransmit-interval>
  giveup-threshold <giveup-threshold>
no
```

Description

This command configures an SSID profile.

The SSID profile configures the SSID. Default WMM mappings exist for all SSIDs. After you customize an WMM mapping and apply it to the SSID, the Mobility Conductor overwrites the default mapping values and uses the user-configured values.

	Description
anti-clogging-token-threshold <anti-clogging-token-threshold>	Simultaneous SAE negotiations above which anti-clogging-token is required.
auth-frame-retransmit-interval	Configure interval between retransmits for SAE Auth frame.

	Description
<auth-frame-retransmit-interval>	20-1000 milliseconds
giveup-threshold <giveup-threshold>	Number of SAE Auth frames transmissions before giving up.
no	Negates any configured parameter.

Example

The following example configures an SSID for WPA2 AES authentication:

```
(host) [md] (config) #wlan sae-profile
(host) [md] (WPA3 SAE Configuration) #
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, except for the noted opmode parameters.	Base operating system, except for the noted parameters.	Config mode on Mobility Conductor.

wlan ssid-profile

```
wlan ssid-profile <profile-name>
  a-basic-rates <mbps>
  a-beacon-rate
  a-tx-rates <mbps>
  advertise-ap-name
  advertise-location
  ageout <seconds>
  auth-req-thresh <auth-req-thresh>
  battery-boost
  cdc-enable
  clone <profile-name>
  deny-bcast
  disable-probe-retry
  dot11r profile
  dtim-period <milliseconds>
  eapol-rate-opt
  edca-parameters-profile {ap|station} <profile-name>
  enforce-user-vlan
  essid <name>
  g-basic-rates <mbps>
  g-beacon-rate
  g-tx-rates <mbps>
  he-ssid-profile
  hide-ssid
  ht-ssid-profile <profile-name>
  local-probe-req-thresh
  max-clients <number>
  max-retries <number>
  max-tx-fail <number>
  mbo-enable
  mcast-rate-opt
  mcast-rate-opt
  mfp-capable
  mfp-required
  multicast-rate
  multiple-tx-replay-counters
  no ...
  okc
  opmode {bSec-128|bSec-256|dynamic-wep|enhanced-open|mpsk-aes|opensystem|static-
wep|wpa-aes|wpa-psk-aes|wpa-psk-tkip|wpa-tkip|wpa2-aes|wpa2-psk-aes|wpa2-psk-
tkip|wpa2-tkip|wpa3-aes-ccm-128|wpa3-aes-gcm-256|wpa3-aes-gcm-256 |wpa3-
cnsa|wpa3-sae-aes|xSec}
  opmode-transition
  qbss-load-enable
  refresh-direction <bidirectional/rx-only/tx-only>
  rts-threshold <number>
  send-transition-disable
  short-preamble
  ssid-enable
  strict-svp
  traffic-steering
  wepkey1 <key>
```

```

wepkey2 <key>
wepkey3 <key>
wepkey4 <key>
weptxkey <index>
wmm
wmm-be-dscp <best-effort>
wmm-bk-dscp <background>
wmm-dscp-mapping
wmm-eap-ac
wmm-ts-min-inact-int <milliseconds>
wmm-uapsd
wmm-vi-dscp <video>
wmm-vo-dscp <voice>
wpa-hexkey <psk>
wpa-passphrase <string>

```

Description

This command configures an SSID profile.

The SSID profile configures the SSID. Default WMM mappings exist for all SSIDs. After you customize an WMM mapping and apply it to the SSID, the Mobility Conductor overwrites the default mapping values and uses the user-configured values.

	Description
<profile-name>	Name of this instance of the profile. The name must be 1-63 characters. default
a-basic-rates	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses. 6, 9, 12, 18, 24, 36, 48, 54 Mbps 6, 12, 24 Mbps
a-beacon-rate	Sets the beacon rate for 802.11a (use for DAS only). Using this parameter in normal operation may cause connectivity problems. default, 6, 9, 12, 18,24,36,48,54 Mbps minimum valid rate
a-tx-rates	Set of 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client. 6, 9, 12, 18, 24, 36, 48, 54 Mbps

	Description
advertise-ap-name	<p>If enabled, APs that are part of this VAP will broadcast AP names in beacon and probe response frames as a part of the vendor-specific Information Element.</p> <p>200 Series, 203H Series, 203R Series, 205H Series, 207 Series, 210 Series, 220 Series, AP-228, and 270 Series do not broadcast AP names in probe response frames.</p> <p>Disabled</p>
advertise-location	<p>If enabled, APs that are part of this VAP will broadcast their GPS coordinates in the beacons and probe response frames as part of a vendor-specific Information Element.</p> <p>Disabled</p>
ageout	<p>Time, in seconds, that a client is allowed to remain idle before being aged out.</p> <p>1000 seconds</p>
auth-req-thresh	<p>The SNR threshold below which incoming authentication requests are ignored. Use this parameter instead of the local probe request threshold parameter to filter out low SNR authentication request.</p> <p>NOTE: Use this parameter with caution. Consult technical support before configuring this parameter.</p> <p>0-100 dB 0 dB</p>
battery-boost	<p>Converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life.</p> <p>NOTE: This parameter requires the PEFNG license. This parameter should not be enabled if you plan on using the Push-To-Talk feature for Polycom SpectraLink devices.</p> <p>Disabled</p>
cdc-enable	<p>Advertizes the Cellular Data Capability (CDC) attribute of an MBO.</p>

	Description
	NOTE: CDC can only be enabled when MBO is enabled.
clone	Name of an existing SSID profile from which parameter values are copied.
deny-bcast	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID. Disabled
disable-probe-retry	Enables or disables battery MAC level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled. NOTE: This parameter is not supported for 200 Series, 210 Series, 220 Series, 270 Series access points. NOTE: Enabled
dot11r-profile	Associates the dot11r-profile with the SSID profile.
dtim-period	Specifies the interval, in beacon periods, between the sending of DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts. 1
eapol-rate-opt	Uses a more conservative rate for more reliable delivery of EAPOL frames. Enabled
edca-parameters-profile	Name of the EDCA profile that applies to this SSID.

	Description
	NOTE: This parameter requires the PEFNG license. Configure this parameter only under the guidance of your Aruba representative.
ap station	Assigns the specified EDCA profile to AP or station (client).
enforce-user-vlan	Enforces data traffic only in user's assigned vlan (Open stations only).
ssid	Name that uniquely identifies a wireless network. The ESSID can be up to 32 characters. If the ESSID includes spaces, you must enclose it in quotation marks.
g-basic-rates	List of supported 802.11b/g rates that are advertised in beacon frames and probe responses. 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps 1, 2 Mbps
g-beacon-rate	Sets the beacon rate for 802.11g (use for DAS only). Using this parameter in normal operation may cause connectivity problems. default, 1,2,5, 6 9, 11, 12, 18, 24, 36, 48, 54 Mbps minimum valid rate
g-tx-rates	Set of 802.11b/g rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client. 1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
he-ssid-profile	Name of high-efficiency SSID profile to use for configuring high-efficiency support. default
hide-ssid	Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security. Disabled
ht-ssid-profile	Name of high-throughput SSID profile to use for configuring high-throughput support. See wlan ht-ssid-profile on page 4179 .

	Description
	default
local-probe-req-thresh	APs will not respond to client probe requests if the SNR value in the probe request is less than the specified threshold value. 0-100 dB 0 dB
max-clients	Maximum number of wireless clients for the AP. This parameter is limited to 1024 clients per radio. Default value for this parameter is the maximum number of clients supported by the AP.
max-retries	Maximum number of retries allowed for the AP to send a frame. 0-15 4
max-tx-fail	The AP assumes the client has left and should be deauthorized when the AP detects this number of consecutive frames were not delivered because the max-retries threshold was exceeded. 0 -2,147,483,647 0
mbo-enable	Enables the Agile Multiband Operations (MBO). Enables the mfp-capable, 802.11k and 802.11u-interworking implicitly on the AP.
mcast-rate-opt	Choose the optimal rate for broadcast/multicast frames.
mcast-rate-opt	Enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate. NOTE: Do not enable this parameter unless instructed to do so by your Aruba technical support representative. Disabled

	Description																																																																				
mfp-capable	<p>When enabled, the SSID supports management frame protection (MFP) capable clients and traditional clients.</p> <p>Disabled</p>																																																																				
mfp-required	<p>When enabled, the SSID only supports MFP capable clients.</p> <p>Disabled</p>																																																																				
multicast-rate	<p>When configured, the Mobility Conductor chooses the rate for video multicast frames. You can configure MCS rates as well. MCS is an important setting because it provides for potentially greater throughput.</p> <p>NOTE: The following information displays the MCS rate if the <code>short-guard-intvl-20MHz</code> parameter in ht-ssid-profile is either enabled or disabled:</p> <table border="1" data-bbox="878 894 1370 1501"> <thead> <tr> <th>MCS SGI</th> <th>Streams</th> <th>20 MHz</th> <th>20 MHz</th> </tr> </thead> <tbody> <tr><td>0</td><td>1</td><td>6.5</td><td>7.2</td></tr> <tr><td>1</td><td>1</td><td>13.0</td><td>14.4</td></tr> <tr><td>2</td><td>1</td><td>19.5</td><td>21.7</td></tr> <tr><td>3</td><td>1</td><td>26.0</td><td>28.9</td></tr> <tr><td>4</td><td>1</td><td>39.0</td><td>43.3</td></tr> <tr><td>5</td><td>1</td><td>52.0</td><td>57.8</td></tr> <tr><td>6</td><td>1</td><td>58.5</td><td>65.0</td></tr> <tr><td>7</td><td>1</td><td>65.0</td><td>72.2</td></tr> <tr><td>8</td><td>2</td><td>13.0</td><td>14.4</td></tr> <tr><td>9</td><td>2</td><td>26.0</td><td>28.9</td></tr> <tr><td>10</td><td>2</td><td>39.0</td><td>43.3</td></tr> <tr><td>11</td><td>2</td><td>52.0</td><td>57.8</td></tr> <tr><td>12</td><td>2</td><td>78.0</td><td>86.7</td></tr> <tr><td>13</td><td>2</td><td>104.0</td><td>115.6</td></tr> <tr><td>14</td><td>2</td><td>117.0</td><td>130.0</td></tr> <tr><td>15</td><td>2</td><td>130.0</td><td>144.4</td></tr> </tbody> </table> <p>NOTE: The MCS rates for video multicast are supported in all 802.11n -capable APs.</p> <p>default, 6, 9, 12, 18, 24, 36, 48, 54 Mbps mcs0-mcs15 default</p>	MCS SGI	Streams	20 MHz	20 MHz	0	1	6.5	7.2	1	1	13.0	14.4	2	1	19.5	21.7	3	1	26.0	28.9	4	1	39.0	43.3	5	1	52.0	57.8	6	1	58.5	65.0	7	1	65.0	72.2	8	2	13.0	14.4	9	2	26.0	28.9	10	2	39.0	43.3	11	2	52.0	57.8	12	2	78.0	86.7	13	2	104.0	115.6	14	2	117.0	130.0	15	2	130.0	144.4
MCS SGI	Streams	20 MHz	20 MHz																																																																		
0	1	6.5	7.2																																																																		
1	1	13.0	14.4																																																																		
2	1	19.5	21.7																																																																		
3	1	26.0	28.9																																																																		
4	1	39.0	43.3																																																																		
5	1	52.0	57.8																																																																		
6	1	58.5	65.0																																																																		
7	1	65.0	72.2																																																																		
8	2	13.0	14.4																																																																		
9	2	26.0	28.9																																																																		
10	2	39.0	43.3																																																																		
11	2	52.0	57.8																																																																		
12	2	78.0	86.7																																																																		
13	2	104.0	115.6																																																																		
14	2	117.0	130.0																																																																		
15	2	130.0	144.4																																																																		

	Description
multiple-tx-replay-counters	Enables Multiple Tx Replay Counters.
no	Negates any configured parameter.
okc	OKC is a similar technique, not defined by 802.11i, available for authentication between multiple APs in a network where those APs are under common administrative control. An Aruba deployment with multiple APs under the control of a single controller is one such example. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys. Enabled
opmode	The layer-2 authentication and encryption to be used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network. opensystem
bSec-128	WPA2 with AES GCM-128 encryption and dynamic keys using 802.1X
bSec-256	WPA2 with AES GCM-256 encryption and dynamic keys using 802.1X
dynamic-wep	WEP with dynamic keys.
enhanced-open	Improved data encryption in open Wi-Fi networks and protects data from sniffing. Enhanced open replaces open system as the default opmode.
mpsk-aes	AES encryption using a pre-shared key.
opensystem	No authentication and encryption.
static-wep	WEP with static keys.
wpa-aes	WPA with AES encryption and dynamic keys using 802.1X.
wpa-psk-aes	WPA with AES encryption using a preshared key.
wpa-psk-tkip	WPA with TKIP encryption using a preshared key.
wpa-tkip	WPA with TKIP encryption and dynamic keys using 802.1X.

	Description
wpa2-aes	WPA2 with AES encryption and dynamic keys using 802.1X.
wpa2-psk-aes	WPA2 with AES encryption using a preshared key.
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1X.
wpa3-aes-ccm-128	WPA3 with AES CCM-128 encryption and dynamic keys using 802.1X.
wpa3-aes-gcm-256	WPA3 with AES GCM-256 encryption.
wpa3-cnsa	WPA3 with AES GCM-256 encryption using CNSA (192 bit).
wpa3-sae-aes	WPA3 with AES encryption using Simultaneous Authentication of Equals.
xSec	Encryption and tunneling of Layer-2 traffic between the managed device and wired or wireless clients, or between managed devices. To use xSec encryption, you must use a RADIUS authentication server. For clients, you must install the Funk Odyssey client software. Requires installation of the xSec license. For xSec between managed devices, you must install an xSec license in each managed device.
opmode-transition	Enables backward compatibility for enhanced open or WPA3-SAE-AES opmodes. Enabled
qbss-load-enable	Enables the AP to advertise the QBSS load element. The element includes the following parameters that provide information on the traffic situation: <ul style="list-style-type: none"> ▪ <code>Station count</code>: The total number of stations associated to the QBSS. ▪ <code>Channel utilization</code>: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel. ▪ <code>Available admission capacity</code>: The remaining amount of medium time

	Description
	<p>(measured as number of 32us/s) available for a station via explicit admission control. The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points.</p> <p>NOTE: Ensure that wmm is enabled for legacy APs to advertise the QBSS load element. For 802.11n APs, ensure that either wmm or high throughput is enabled.</p> <p>Disabled</p>
refresh-direction	The refresh direction of WLAN SSID profile.
<bidirectional>	Bidirectional data frames that are used for station refresh.
<rx-only>	<p>Received data frames that are used for station refresh.</p> <p>NOTE: The receive-only mode does not use null frames for station refresh.</p>
<tx-only>	Transmitted data frames that are used for station refresh.
rts-threshold	Wireless clients transmitting frames larger than this threshold must issue RTS and wait for the AP to respond with CTS. This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting. 2333 bytes
send-transition-disable	Send Transition-Disable KDE to WPA3 clients.
short-preamble	<p>Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.</p> <p>Enabled</p>
strict-svp	Enable Strict Spectralink Voice Protocol (SVP)

	Description
	Disabled
traffic-steering	If enabled, traffic steering is done for EAP-SIM/EAP-AKA clients that are connected to this SSID.
wepkey1 - wepkey4	Static WEP key associated with the key index. Can be 10 or 26 hex characters in length.
wepkey	Key index that specifies which static WEP key is to be used. 1, 2, 3, 4 1
wmm	Enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function. WMM provides prioritization of specific traffic relative to other traffic in the network. Disabled
wmm-be-dscp	DSCP value used to map WMM best-effort traffic. 0-63
wmm-bk-dscp	DSCP used to map WMM background traffic. 0-63
wmm-dscp-mapping	Enables or disables WMM map to GRE DSCP in D-Tunnel upstream direction.
wmm-eap-ac {background best-effort default video voice}	Override the WMM Access Class (AC) of EAP traffic.
wmm-ts-min-inact-int	Specifies the minimum inactivity time-out threshold of WMM traffic. This setting is useful in environments where low inactivity interval timeouts are advertised, which may cause unwanted timeouts. 0-3,600,000 milliseconds 0 milliseconds
wmm-uapsd	Enable WMM UAPSD powersave. Enabled
wmm-vi-dscp	DSCP used to map WMM video traffic. 0-63

	Description
wmm-vo-dscp	DSCP used to map WMM voice traffic. 0-63
wpa-hexkey	WPA PSK.
wpa-passphrase	WPA passphrase with which to generate a PSK.

Suite-B Cryptography

The `opmode` parameters for Suite-B encryption, `wpa2-aes-gcm-128` and `wpa2-aes-gcm-256`, require the ACR license. All 7000 Series and 7200 Series support Suite-B encryption.

Multicast Rate Optimization

The Multicast Rate Optimization feature dynamically selects the rate for sending broadcast/multicast frames on any BSS. This feature determines the optimal rate for sending broadcast and multicast frames based on the lowest of the unicast rates across all associated clients.

When the Multicast Rate Optimization option ([mcast-rate-opt](#)) is enabled, the Mobility Conductor scans the list of all associated stations in that BSS and finds the lowest transmission rate as indicated by the rate adaptation state for each station. If there are no associated stations in the BSS, it selects the lowest configured rate as the transmission rate for broadcast and multicast frames.

This feature is disabled by default. Multicast Rate Optimization applies to broadcast and multicast frames only. 802.11 management frames are not affected by this feature and will be transmitted at the lowest configured rate.



The Multicast Rate Optimization feature should only be enabled on a BSS where all associated stations are sending or receiving unicast data. If there is no unicast data to or from a particular station, then the rate adaptation state may not accurately reflect the current sustainable transmission rate for that station. This could result in a higher packet error rate for broadcast or multicast packets at that station.

Example

The following example configures an SSID for WPA2 AES authentication:

```
(host) [md] (config) #wlan ssid-profile corpnet
(host) [md] (SSID Profile "corpnet") #essid Corpnet
(host) [md] (SSID Profile "corpnet") #opmode wpa2-aes
```

Command History

Release	Description
ArubaOS 8.7.0.0	The <code>advertise-ap-name</code> parameter was modified to include AP names in probe response frames.
ArubaOS 8.6.0.0	The following parameters were added: <ul style="list-style-type: none"> ▪ <code>cdc-enable</code> ▪ <code>mbo-enable</code>
ArubaOS 8.5.0.0	The <code>refresh-direction</code> parameter was added. The <code>wpa3-aes-gcm-256</code> sub-parameter to the <code>opmode</code> parameter was added.
ArubaOS 8.4.0.0	The following sub-parameters to the <code>opmode</code> parameter and the <code>opmode-transition</code> parameter were added: <ul style="list-style-type: none"> ▪ <code>enhanced-open</code> ▪ <code>mpsk-aes</code> ▪ <code>opensystem</code> ▪ <code>wpa3-aes-ccm-128</code> ▪ <code>wpa3-cnsa</code> ▪ <code>wpa-sae-aes</code>.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, except for the noted <code>opmode</code> parameters.	Base operating system, except for the noted parameters.	Config mode on Mobility Conductor.

wlan traffic-management-profile

```
wlan traffic-management-profile <profile-name>
  bw-alloc virtual-ap <virtual-ap> share <percent>
  clone <profile-name>
  no ...
  report-interval <minutes>
  shaping-policy default-access|fair-access|preferred-access
```

Description

This command configures a traffic management profile.

The traffic management profile allows you to allocate bandwidth to SSIDs. When you enable the band-steering feature, an AP keeps track of all BSSIDs active on a radio, all clients connected to the BSSID, and 802.11a/g, 802.11b, or 802.11n capabilities of each client. Every sampling period, airtime is allocated to each client, giving it opportunity to get and receive traffic. The specific amount of airtime given to an individual client is determined by;

- Client capabilities (802.11a/g, 802.11b or 802.11n)
- Amount of time the client spent receiving data during the last sampling period
- Number of active clients in the last sampling period
- Activity of the current client in the last sampling period

The `bw-alloc` parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP.

Parameter	Description	Range	Default
<profile-name>	Name of this profile. 1-63 characters. default	—	default
bw-alloc	Minimum bandwidth, as a percentage of available bandwidth, allocated to a Virtual AP when there is congestion on the wireless network. An virtual AP can use all available bandwidth if no other virtual APs are active.		
virtual-ap <virtual-ap>	Name of the virtual AP to which you will allocate a share of bandwidth.	—	—

Parameter	Description	Range	Default
share <percent>	Percentage of available bandwidth allocated to this virtual AP. 0-100	0-100	—
clone <profile-name>	Name of an existing traffic management profile from which parameter values are copied.	—	—
no	Negates any configured parameter.	—	—
report-interval <minutes>	Number of minutes between bandwidth usage reports. 1 - 999999 minutes 5 minutes	1 - 999999 minutes	5 minutes
shaping-policy	Defines the Station Shaping Policy This feature has the following three options: <ul style="list-style-type: none"> ■ default-access: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. ■ fair-access: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The bw-alloc parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP. ■ preferred-access: High- 	default-access fair-access preferred-access	default-access

Parameter	Description	Range	Default
	<p>throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.</p> <p>default-access, fair-access, preferred-access</p> <p>default-access</p>		

Example

The following example configures a traffic management profile that allocates bandwidth to the corpnet virtual AP:

```
(host) [md] (config) #wlan traffic-management-profile best
(host) [md] (Traffic management profile "best") #bw-alloc virtual-ap corpnet
share 75
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan tsm-req-profile

```
wlan tsm-req-profile <profile-name>  
  bin0-range <bin0-range>  
  clone  
  dur-mandatory  
  measure-duration <measure-duration>  
  no  
  num-repeats <num-repeats>  
  random-interval <random-interval>  
  request-mode {normal | triggered}  
  traffic-id <traffic-id>
```

Description

This command configures a TSM Report Request Profile.

The tsm-req-profile is a part of the 802.11K profile. It is used to configure the parameters for the Transmit Stream or Category Measurement frames. It takes effect only when the 802.11K feature is enabled.

Parameter	Description
<profile-name>	Name of this profile. The name must be 1-63 characters. default
bin0-range <bin0-range>	This value is used to set the 'Bin 0 Range' field in the Transmit Stream or Category Measurement Request frame. Bin 0 Range indicates the delay range of the first bin (Bin 0) of the Transmit Delay Histogram, expressed in units of TUs. 0- 255 6
clone <source>	Creates a copy of the Transmit Stream Measurement Request Report Request Profile. <source> is the name of an existing TSM Profile from which parameter values are copied.
dur-mandatory	This parameter is used to set the "Duration Mandatory" bit of the Measurement Request Mode field of the Transmit Stream or Category Measurement Request frame. Enabled

Parameter	Description
<code>measure-duration <measure-duration></code>	<p>This parameter is used to set the Measurement Duration field in the Transmit Stream or Category Measurement Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs. When the request mode for the Transmit Stream or Category Measurement Request frame is set to triggered, the Measurement Duration field should be set to 0.</p> <p>0- 65535 9776</p>
<code>no</code>	<p>Negates any configured parameter</p>
<code>num-repeats <num-repeats></code>	<p>This parameter is used to set the Number of Repetitions field in the Transmit Stream or Category Measurement Request frame. The Number of Repetitions field contains the requested number of repetitions for all the Measurement Request elements in this frame. A value of zero in the Number of Repetitions field indicates Measurement Request elements are executed once without repetition. A value of 65535 in the Number of Repetitions field indicates Measurement Request elements are repeated until the measurement is canceled or superseded.</p> <p>0-65535 65535</p>
<code>random-interval <random-interval></code>	<p>This parameter is used to set the Randomization Interval field in the Transmit Stream or Category Measurement Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units). When the request mode for the Transmit Stream or Category Measurement Request frame is set to "triggered", the Randomization Interval is not used and is set to 0. A Randomization Interval of 0 in a measurement request indicates that no random delay is to be used.</p> <p>0-65535 0</p>
<code>request-mode {normal triggered}</code>	<p>This parameter is used to determine the request mode for the Transmit Stream or Category Measurement Request frame.</p> <p>normal, triggered normal</p>

Parameter	Description
traffic-id <traffic-id>	<p>The parameter is used to set the Traffic Identifier field in the Transmit Stream or Category Measurement Request frame. The Traffic Identifier field contains the TID subfield. The TID subfield indicates the TC or TS for which traffic is to be measured.</p> <p>0-255</p> <p>96</p>

Example

The following example configures a TSM Report Request Profile:

```
(host) [md] (config) #wlan tsm-req-profile default
(host) [md] (TSM Report Request Profile "default") #bin0-range 1
(host) [md] (TSM Report Request Profile "default") #dur-mandatory
(host) [md] (TSM Report Request Profile "default") #measure-duration 25
(host) [md] (TSM Report Request Profile "default") #num-repeats 0
(host) [md] (TSM Report Request Profile "default") #random-interval 0
(host) [md] (TSM Report Request Profile "default") #request-mode normal
(host) [md] (TSM Report Request Profile "default") #traffic-id 96
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Conductor.

wlan virtual-ap

```
wlan virtual-ap <profile-name>
  aaa-profile <profile-name>
  allowed-5g-radio {all|first-5g-radio-only|second-5g-radio-only}
  allowed-band <band>
  allowed-band-6ghz
  anyspot-profile <profile>
  auth-failure-blacklist-time / auth-failure-denylist-time <seconds>
  band-steering
  blacklist/denylist
  blacklist-time / denylist-time <seconds>
  broadcast-filter all|arp
  cellular-handoff-assist
  clone <profile-name>
  deny-inter-user-traffic
  deny-time-range <range>
  disable-on-6ghz-mesh
  dos-prevention
  dot11k-profile
  dynamic-mcast-optimization
  dynamic-mcast-optimization-threshold
  fdb-update-on-assoc
  forward-mode {tunnel|bridge|split-tunnel|decrypt-tunnel}
  ftm-responder-enable
  ha-disc-onassoc
  hs2-profile
  mobile-ip
  no ...
  openflow-enable
  preserve-vlan
  rap-operation {always|backup|persistent|standard}
  ssid-profile <profile-name>
  steering-mode band-balancing|force-5ghz|prefer-5ghz
  strict-compliance
  vap-enable
  vlan <vlan>...
  vlan-mobility
  wan-operation
  wmm-traffic-management-profile
```

Description

This command configures a virtual AP profile.



The WMM traffic management feature is not supported on AP-203H, AP-203R, AP-203RP, AP-207, AP-228, AP-277, 200 Series, 210 Series, 220 Series, 340 Series, 500 Series, 510 Series access points.

WLAN profiles configure WLANs in the form of virtual AP profiles. A virtual AP profile contains an SSID profile which defines the WLAN and an AAA profile which defines the authentication for the

WLAN. You can configure and apply multiple instances of virtual AP profiles to an AP group or to an individual AP.

A named VLAN can be deleted although it is configured in a virtual AP profile. If this occurs the virtual AP profiles becomes invalid. If the named VLAN is added back later the virtual AP becomes valid again.

The `broadcast-filter arp` parameter is enabled by default. If your Mobility Conductor supports clients behind a wireless bridge or virtual clients on VMware devices, you must disable the `broadcast-filter arp` setting to allow those clients to obtain an IP address. In previous releases of ArubaOS, the virtual AP profile included two unique broadcast filter parameters; the `broadcast-filter all` parameter, which filtered out all broadcast and multicast traffic in the air except DHCP response frames (these were converted to unicast frames and sent to the corresponding client) and the `broadcast-filter arp` parameter, which converted broadcast ARP requests to unicast messages sent directly to the client.

The **broadcast-filter arp** setting includes the additional functionality of `broadcast-filter all` parameter, where DHCP response frames are sent as unicast to the corresponding client. This can impact DHCP discover or requested packets for clients behind a wireless bridge and virtual clients on VMware devices. Disable the `broadcast-filter arp` setting using the `wlan virtual-ap <profile> no broadcast-filter arp` command to resolve this issue and allow clients behind a wireless bridge or VMware devices to receive an IP address.

If there is only one VLAN defined, then the Mobility Conductor will send IPv6 RAs as usual. If, however, there are multiple VLANs, then the Mobility Conductor will automatically convert 802.11 multicast frames to unicast. This conversion prevents RA frames from being sent with a multicast key to all clients on the BSSID, which could lead to clients having multiple IPv6 addresses.

Parameter	Description
<code><profile-name></code>	Name of this profile. 1-63 characters default
<code>aaa-profile</code>	Name of the AAA profile that applies to this virtual AP. default
<code>allowed-5g-radio</code>	The 5 GHz radio(s) on which to configure the virtual AP: <ul style="list-style-type: none">■ all—dual 5 GHz band only■ first-5g-radio-only—first 5 GHz band only■ second-5g-radio-only—second 5 GHz band only

Parameter	Description
	<p>all</p> <p>NOTE: This parameter is ignored if the AP has only one 5 GHz radio.</p>
allowed-band	<p>The band(s) on which to use the virtual AP:</p> <ul style="list-style-type: none"> ■ a—5 GHz band only (802.11a) ■ g—2.4 GHz band only (802.11b/802.11g) ■ all—both 2.4 GHz and 5 GHz bands (802.11a and 802.11b/802.11g) ■ none—disable both 2.4 GHz and 5 GHz bands <p>all</p> <p>NOTE: The none option is supported from ArubaOS 8.9.0.0 or later versions.</p>
allowed-band-6ghz (ArubaOS 8.9.0.0 or later versions)	<p>Enable 6 GHz band to use the virtual AP.</p> <p>NOTE: This field is applicable to Wi-Fi 6E APs only.</p>
anyspot-profile	<p>Anyspot Profile associated with this Virtual AP Profile. The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.</p>
auth-failure-blacklist-time / auth-failure-denylist-time	<p>Time, in seconds, a client is blocked if it fails repeated authentication. A value of 0 blocks a client indefinitely.</p> <p>0-2,147,483,647 seconds 0</p>

Parameter	Description
band-steering	<p>ARM's band steering feature can encourage or require dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.</p> <p>The band steering feature supports three steering modes, which can be configured via the steering-mode parameter:</p>

Parameter	Description
	<p>Band steering can be configured on both campus APs and remote APs that have a virtual AP profile set to tunnel, decrypt-tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs has virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual AP in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that also have bridge or split-tunnel virtual APs only.</p> <p>disabled</p>
blacklist/denylist	<p>Enables detection of DoS attacks, such as ping or SYN floods, that are not spoofed death attacks.</p> <p>enabled</p>
blacklist-time/denylist-time	<p>Number of seconds that a client is quarantined from the network after being blocked.</p> <p>0-2,147,483,647 seconds 3600 seconds (1 hour)</p>
broadcast-filter	<p>Filter out broadcast and multicast traffic in the air.</p> <ul style="list-style-type: none"> ■ all <p>NOTE: Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the managed device, so the managed</p>

Parameter	Description
	<p>device is able to drop all broadcast traffic. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the managed device is not able to filter out that broadcast traffic.</p> <p>IMPORTANT: If you enable this option, you must also enable the <code>Broadcast-Filter ARP</code> parameter in the stateful firewall configuration to prevent ARP requests from being dropped. Note also that although a virtual AP profile can be replicated from a Mobility Conductor to managed device, stateful firewall settings do not. If you select the broadcast-filter all option for a Virtual AP Profile on a Mobility Conductor, you must enable the broadcast-filter arp setting on each individual managed device.</p> <ul style="list-style-type: none"> ■ <code>arp</code> <p>If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the <code>show ap active</code> and the <code>show datapath tunnel</code> command. If enabled, the output will display the letter a in the flags column.</p>

Parameter	Description
	<p>Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the managed device, so the managed device is able to convert ARP requests directed to the broadcast address into unicast. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the managed device is not able to convert that broadcast traffic.</p> <p>all, arp</p> <p>For the option all, the default value is disabled.</p> <p>For the option arp, the default value is enabled.</p>
cellular-handoff-assist	<p>When both the client match and cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G or 4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G or 4G radio that provides better network access. This feature is disabled by default, and is recommended only for Wi-Fi hotspot deployments.</p> <p>disabled</p>
clone	<p>Name of an existing traffic management profile from which parameter values are copied.</p>

Parameter	Description
deny-inter-user-traffic	<p>Select this check box to deny traffic between the clients using this virtual AP profile.</p> <p>The <code>firewall</code> command includes an option to deny all inter-user traffic, regardless of the Virtual AP profile used by those clients.</p> <p>If the global setting to deny inter-user traffic is enabled, all inter-user traffic between clients will be denied, regardless of the settings configured in the virtual AP profiles. If the setting to deny inter-user traffic is disabled globally but enabled on an individual virtual ap, only the traffic between untrusted users and the clients on that particular virtual AP will be blocked.</p>
deny-time-range	<p>Specify the name of the time range for which the AP will deny access. Time ranges can be defined using the CLI command time-range.</p>
disable-on-6ghz-mesh (ArubaOS 8.9.0.0 or later versions)	<p>If enabled, virtual AP is disabled on 6 GHz band only when AP is provisioned as mesh.</p> <p>NOTE: This field is applicable to Wi-Fi 6E APs only.</p>
dos-prevention	<p>If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.</p> <p>disabled</p>

Parameter	Description
dot11k-profile	Name of an 802.11k profile to be associated with this VAP. default
dynamic-mcast-optimization	Enable or /Disable dynamic multicast optimization. This parameter can only be enabled on a managed device with a PEFNG license. disabled
dynamic-mcast-optimization-threshold	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops. 2-255 stations 6 stations
fdb-update-on-assoc	This parameter enables seamless failover for silent clients, allowing them to re-associate. If you select this option, the managed device will generate a Layer 2 update on behalf of client to update forwarding tables in bridge devices. disabled
forward-mode	Controls whether 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). Select one of the following forward modes:

Parameter	Description
	<ul style="list-style-type: none"><li data-bbox="1133 268 1399 793">■ Tunnel: When an AP is in tunnel forwarding mode, the AP handles all 802.11 association requests and responses. The AP sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual.<li data-bbox="1133 800 1399 1381">■ Bridge: When an AP is in bridge mode, data is bridged onto the local Ethernet LAN. When in bridge mode, the AP handles all 802.11 association requests and responses, encryption or decryption processes, and firewall enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode supports only the 802.1X authentication type.<li data-bbox="1133 1388 1399 1780">■ Split-Tunnel: Data frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). The AP handles all 802.11 association requests and responses, encryption or decryption, and firewall

Parameter	Description
	<p>enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in split-tunnel mode supports only the 802.1X authentication type.</p> <ul style="list-style-type: none"> ■ Decrypt-Tunnel: An AP in decrypt-tunnel forwarding mode decrypts and decapsulates all 802.11 frames from a station and sends the 802.3 frames through the GRE tunnel to the managed device, which then applies firewall policies to the user traffic. This mode allows a network to utilize the encryption or decryption capacity the AP while reducing the demand for processing resources on the managed device. APs in decrypt-tunnel forwarding mode also manage all 802.11 association requests and responses, and process all 802.11e and 802.11k action frames. <p>NOTE: Virtual APs in bridge or split-tunnel mode using static WEP should use key slots 2-4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.</p> <p>tunnel, bridge. split-tunnel decrypt-tunnel tunnel</p>

Parameter	Description
ftm-responder-enable	<p>Enables 802.11mc Fine Timing Measurement (FTM) on radio (responder mode only).</p> <p>This feature is supported on 500 Series, 500H Series, 510 Series, 530 Series, 550 Series, 560 Series, 570 Series, 630 Series, and 650 Series access points.</p> <p>disabled</p>
ha-disc-onassoc	<p>If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practices is to leave this parameter disabled, as it increases IP mobility control traffic between managed devices in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients.</p> <p>NOTE: <code>ha-disc-onassoc</code> parameter works only when IP mobility is enabled and configured on the managed device.</p> <p>disabled</p>
hs2-profile	<p>Enables or disables a hotspot profile.</p> <p>enabled</p>

Parameter	Description
mobile-ip	Enables or disables IP mobility on a virtual AP. This is enabled by default. L3 mobility service is active on a VAP only if router mobile is also enabled on the managed device. enabled
no	Negates any configured parameter.
openflow-enable	Enables OpenFlow on AP forwarding path.
preserve-vlan	This parameter allows clients to retain their previous VLAN assignment if the client disassociates from an AP and then immediately re-associates either with same AP or another AP on same managed device.
rap-operation	Configures when the virtual AP operates on a remote AP: <ul style="list-style-type: none"> ■ always— Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ backup—Enables the virtual AP if the remote AP cannot connect to the managed device (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ persistent— Permanently enables the virtual AP after the remote AP initially connects to the managed device (Bridge Mode only). This option can be used for any (Open or

Parameter	Description
	<p>PSK or 802.1X) bridge VAPs.</p> <ul style="list-style-type: none"> ■ standard—Enables the virtual AP when the remote AP connects to the managed device. This option can be used for any (bridge or split-tunnel or tunnel or d-tunnel) VAPs. <p>always, backup, persistent, standard standard</p>
ssid-profile	<p>Name of the SSID profile that applies to this virtual AP.</p> <p>default</p>
steering-mode	<p>Band steering supports three different band steering modes.</p> <ul style="list-style-type: none"> ■ Force-5GHz: When the AP is configured in force-5GHz band steering mode, the AP will try to force 5 GHz-capable APs to use that radio band. ■ Prefer-5GHz (Default): If you configure the AP to use prefer-5GHz band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. ■ Balance-bands: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that

Parameter	Description
	<p>the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz while the 2.5 GHz band operates in 20 MHz.</p> <p>NOTE: Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default prefer-5GHz steering mode available in ArubaOS 6.0 and later.</p> <p>Force-5 GHz, prefer-5 GHz, balance-bands prefer-5 GHz</p>
strict-compliance	<p>If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.</p> <p>disabled</p>
vap-enable	<p>Enable or disable the virtual AP.</p> <p>enabled</p>

Parameter	Description
vlan	<p>The VLAN(s) into which users are placed in order to obtain an IP address. Enter VLANs as a comma-separated list of existing VLAN IDs or VLAN names. A mixture of names and numeric IDs are not allowed.</p> <p>NOTE: You must add an existing VLAN ID to the Virtual AP profile.</p> <p>1</p>
vlan-mobility	<p>VLAN mobility retains the client VLAN on roaming irrespective of the VAP VLAN, provided the user VLANs are extended. VLAN mobility and mobile IP are mutually exclusive. VLAN mobility does not reuse user firewall sessions on roaming as the sessions will have to be recreated locally on the roamed managed device.</p> <p>disabled</p>
wan-operation	<p>Specify the wan-operation to enable Virtual AP depending on the state of the WAN link.</p> <p>always, backup, primary always</p>
wmm-traffic-management-profile	<p>Specify the WMM Traffic Management Profile to be associated with this Virtual AP Profile.</p>

Example

The following example configures a virtual AP.

```
(host) [md] (config) #wlan virtual-ap corpnet
(host) [md] (Virtual AP profile "corpnet") #vlan 1
```

```
(host) [md] (Virtual AP profile "corpnet") #aaa-profile corpnet
(host) [md] (Virtual AP profile "corpnet") #ftm-enable
```

The following example configures 802.11mc FTM responder.

```
(host) [node] (config) #wlan virtual-ap test
(host) [node] (Virtual AP profile "test") #ftm-responder-enable
(host) [node] (Virtual AP profile "test") #write mem
```

The following example configures the parameters for a 6 GHz band (ArubaOS 8.9.0.0 or later versions).

```
(host) [mynode] (config) #wlan virtual-ap <profile>
(host) [mynode] (Virtual AP profile "profile") #vap-enable
(host) [mynode] (Virtual AP profile "profile") #vlan <vlan-id>
(host) [mynode] (Virtual AP profile "profile") #allowed-band-6ghz
(host) [mynode] (Virtual AP profile "profile") #disable-on-6ghz-mesh
```

Command History

Version	Modification
ArubaOS 8.9.0.0	The following changes were made: <ul style="list-style-type: none"> ■ The <code>allowed-band-6ghz</code> and <code>disable-on-6ghz-mesh</code> parameters were introduced. ■ The none option was added under <code>allowed-band</code> parameter. ■ All instances of <code>blacklist</code> have been replaced with <code>denylist</code>.
ArubaOS 8.8.0.0	The <code>ftm-responder-enable</code> parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wlan wmm-traffic-management-profile

```
wlan wmm-traffic-management-profile <profile-name>  
  background <share>  
  best-effort <share>  
  clone <source>  
  enable-shaping  
  no  
  video <share>  
  voice <share>
```

Description

This command configures bandwidth shaping for WMM access categories.

Bandwidth shaping is only applied on the down-link traffic.

The bandwidth share percentage configuration for WMM traffic management is not supported on 203H Series, 203R Series, 207 Series, 270 Series, 200 Series, 210 Series, 220 Series, AP-228, 340 Series, 500 Series, 510 Series, 570 Series, and AP-518 access points. Therefore, the following parameters do not take effect in these AP platforms: **background<share>**, **best-effort-share <share>**, **video<share>**, and **voice<share>**.



After you configure the WMM traffic management profile, apply it to the virtual AP profile. For WMM traffic management to take effect, you must enable `fair-access` or `preferred-access` parameter under [wlan traffic-management-profile](#).

Parameter	Description
<code>background <share></code>	Bandwidth allocation, in percentage (%), for WMM background access traffic category. 0-100% 5%
<code>best-effort <share></code>	Bandwidth allocation, in percentage (%), for WMM best effort access traffic category. 0-100% 5%
<code>clone <source></code>	Copies the configuration from another WMM Traffic management profile.
<code>enable-shaping</code>	Enables a bandwidth shaping policy so that the allocated bandwidth share is appropriately used. disabled

Parameter	Description
no	Negates any configured parameter.
video <share>	Bandwidth allocation, in percentage (%), for video access traffic category. 0-100% 55%
voice <share>	Bandwidth allocation, in percentage (%), for voice access traffic category. 0-100% 35%

Example

The following example configures a WMM traffic management profile:

```
(host) [md] (config) #wlan wmm-traffic-management-profile test
(host) [md] (WMM Traffic management profile "test") #enable-shaping
(host) [md] (WMM Traffic management profile "test") #background 7
(host) [md] (WMM Traffic management profile "test") #best-effort 10
(host) [md] (WMM Traffic management profile "test") #voice 40
(host) [md] (WMM Traffic management profile "test") #video 43
```

Apply the WMM traffic management profile to the virtual AP profile:

```
(host) [md] (config) #wlan virtual-ap employee
(host) [md] (Virtual AP profile "employee") #wmm-traffic-management-profile
test
```

Enable the `fair-access` or `preferred access` parameter under `wlan traffic-management-profile`:

```
(host) [md] (config) #wlan traffic-management-profile test
(host) [md] (Traffic management profile "test") #shaping-policy fair-access
OR
(host) [md] (Traffic management profile "test") #shaping-policy preferred-
access
```

Apply the traffic management profile to an ap group:

```
(host) [md] (config) #ap-group default
(host) [md] (AP group "default") #dot11a-traffic-mgmt-profile test
```


Related Commands

Command	Description
show wlan wmm-traffic-management-profile	Displays the WMM traffic management profile(s) configured on the managed device.
wlan traffic-management-profile	Configures a traffic management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Conductor.

wmm-dscp-mapping

wmm-dscp-mapping

Description

This command enables or disables WMM DSCP map in the upstream direction decrypt-tunnel mode.

The WMM DSCP map is enabled by default. Use the **no** form of this command to disable the WMM DSCP map.

Example

The following example enables WMM DSCP mapping:

```
(host) [mynode] (config) #wmm-dscp-mapping
```

The following example disables WMM DSCP mapping:

```
(host) [mynode] (config) #no wmm-dscp-mapping
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

wms ap

```
wms ap <bssid> mode {suspected-rogue <confidence-level>} [{interfering|manually-  
contained|neighbor|rogue|valid}<add|resend|source>]
```

Description

This command allows you to classify an AP into one of the several categories.

If AP learning is enabled (with the `ids-wms-general-profile learn-ap` command), non-Aruba APs connected on the same wired network as Aruba APs are classified as valid APs. If AP learning is disabled, a non-Aruba AP is classified as an unsecure or suspect-unsecure AP.

Parameter	Description
<bssid>	BSSID of the AP.
mode	Classify the AP into one of the following categories.
suspected-rogue	A suspected rogue AP that is plugged into the wired side of the network but may not be an unauthorized device. Automatic shutdown of rogue APs does not apply to these devices.
<confidence-level>	The confidence level setting for the suspected rogue AP.
interfering	An AP seen in the RF environment but is not connected to the wired network.
manually-contained	Manually enables denial of service from this AP
neighbor	An neighboring AP whose BSSID is known.
rogue	A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.
valid	An AP that is part of the enterprise providing WLAN service.
<add>	Create an entry, if not already present, for the AP classification mode.
<resend>	Resend the mode even if there is no change.
<source>	The source of the manual reclassification. Select one of the following: <ul style="list-style-type: none">■ admin: Manual reclassification is done from the CLI.■ amp: Manual reclassification is done from AirWave.■ restapi: Manual reclassification is done from the REST API.■ webui: Manual reclassification is done from the WebUI. admin

Examples

The following example classifies an interfering AP:

```
(host) [mynode] #wms ap 01:00:00:00:00:00 mode interfering
```

The following example assigns manual reclassification source to the monitored AP:

```
(host) [mynode] #wms ap 80:8d:b7:80:da:74 mode valid source admin
```

Command History

Release	Modification
ArubaOS 8.8.0.0	The <source> sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms clean-db

wms clean-db

Description

This command deletes all entries from the WMS database.

Do not use this command unless instructed to do so by an Aruba representative.

Parameter	Description
clean-db	Cleans the WMS database.

Example

The following example deletes the WMS database:

```
(host) [mynode] #wms clean-db  
WMS Database will be deleted. Do you want to proceed with this action [y/n]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms client

```
wms client <mac>  
  mode {interfering|manually-contain|valid}  
  valid-exempt {insert|remove}
```

Description

This command allows you to classify a wireless client into one of several categories.

ArubaOS can automatically determine client classification based on client behavior, but this command allows you to explicitly classify a client. The classification of a client is used in certain policy enforcement features. For example, if **protect-valid-sta** is enabled in the IDS Unauthorized Device Profile, then clients that are classified as valid cannot connect to non-valid APs.

Parameter	Description
<mac>	MAC address of the client.
mode	Classifies the client into one of the following categories:
interfering	Setting the client mode to <i>interfering</i> makes it part of clients outside the enterprise
manually-contain	Manually enables denial of service to this client.
valid	A client that is part of the enterprise.
valid-exempt	Classifies the client under this option to exempt from Valid Station Protection and Valid Station Misassociation Detection.
insert	Adds the client to the valid-exempt list and exempt from Valid Station Protection and Valid Station Misassociation Detection. If the client exists in the WMS, the classification is set to valid. In case the client does not exist in the WMS, a client entry is created and then the classification is set to valid.
remove	Removes the client from the list of valid-exempt clients.

Example

The following example classifies a client as valid:

```
(host) [mynode] #wms client 00:00:A4:34:C9:B3 mode valid
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms export-class

```
wms export-class <filename>
```

Description

This command exports classification information into a file.

This command writes classification data into comma separated values (CSV) files—one for APs and one for clients. You can import these files into the Aruba Mobility Manager system.

Parameter	Description
<filename>	Name of the file into which you want to export classification information.

Example

The following example exports classification data into an AP and a client file:

```
(host) [mynode] #wms export-class class
Exported data to class_ap.csv and class_sta.csv
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms export-db

```
wms export-db <filename>
```

Description

This command exports the WMS database to a specified file. The file is exported as an ASCII text file.

Parameter	Description
<filename>	Name of the file into which you want to export the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Example

The following example exports the WMS database to a file:

```
(host) [mynode] #wms export-db database
Exported WMS DB to database
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms fix-db

```
wms fix-db
  table
    ap
    client
    probe
```

Description

This command addresses some types of WMS database corruption.

Parameter	Description
table	Address WMS database table corruption issues for one of the following: <ul style="list-style-type: none">▪ ap: The database table containing monitored AP data.▪ client: The database table containing monitored client data.▪ probe: The database table containing deployed AP data.

Example

The following example exports the WMS database to a file:

```
(host) [mynode] #wms fix-db table ap
This command will try to fix corruption in the WMS database.
This may take several minutes, so it is recommended to run this in off-peak
hours.
Do you want to proceed with this action [y/n]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms import-db

```
wms import-db <filename>
```

Description

This command imports the specified file into the WMS database. The imported file replaces the WMS database. The imported file must be a valid WMS database file that you previously exported using the `wms export-db` command.

Parameter	Description
<filename>	Name of the file into which you want to import into the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Example

The following example imports the WMS database from a file:

```
(host) [mynode] #wms import-db database
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms reinit-db

wms reinit-db

Description

This command reinitializes the WMS database to its factory default setting. When you use this command, there is no automatic backup of the current database.

Example

The following example reinitializes the WMS database:

```
(host) [mynode] #wms reinit-db  
WMS Database will be re-initialized. Do you want to proceed with this action  
[y/n ]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms restart-snapshot

```
wms restart-snapshot {ap|rogue-ap|sta}
```

Description

This command restarts periodic snapshot messaging by the WLAN Management System (WMS).

Parameter	Description
ap	Restarts the monitored AP snapshot.
rogue-ap	Restarts the monitored rogue AP snapshot.
sta	Restarts the monitored client snapshot.

Example

The following example restarts snapshot messaging for monitored APs:

```
(host) [mynode] #wms restart-snapshot ap
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Conductor.

wms test

```
wms test {busy <interval>|lc-poll-interval <interval-time>}
```

Description

This command configures WLAN Management System (WMS) test settings.

Parameter	Description
busy <interval>	Sets a time interval, in seconds, that the WMS is busy.
lc-poll-interval <interval-time>	Sets a polling interval, in minutes, for communication between the WMS and managed devices. The time interval must be between 10-360 minutes.

Example

The following example sets a polling interval of 15 minutes:

```
(host) [mynode] (config) #wms test lc-poll-interval 15
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Conductor.

write

```
write {erase [all]|memory|terminal}
```

Description

This command saves the running configuration to memory when the **memory** parameter is used or displays the running configuration on the screen when the **terminal** parameter is used. This command can also be used to erase the running configuration by using the **erase** parameter. For more information about how to return the device to a factory default state, see [wipe](#) command.

Parameter	Description
erase	Erases the running system configuration file. If you specify all , the configuration and all data in controller databases (including the license, WMS, and internal databases) are erased. Starting from ArubaOS 8.11.0.0, the write erase and write erase all commands can be issued only from the /mm and /mm/mynode nodes of the controller.
memory	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.
terminal	Displays the current system configuration.

Configuration changes made using the CLI affect only the current session. You must save your changes for them to be retained across system reboots. Changes are lost if the system reboots before saving the changes. To save your configuration changes, use the `write memory` command.

If you use the `write erase` command, the license key management database on the controller is not affected. If you use the `write erase all` command, all databases on the controller are deleted, including the license key management database. If you reset the controller using this command, perform the Initial Setup as described in the *ArubaOS Quick Start Guide*.

If you use the `write terminal` command, all of the commands used to configure controller appear on the terminal. If paging is enabled, there is a pause mechanism that stops the output from printing continuously to the terminal. To navigate through the output, use any of the commands displayed at the bottom of the output, as described below. If paging is disabled, the output prints continuously to the terminal. For more information about the `paging` command, see [paging on page 1069](#).

Key	Description
Q	Exit the display.

Key	Description
U	Page up through the output.
spacebar	Page down through the output.
/	Enter a text string to search for.
N	Repeat the text string to search for.

Example

The following example saves your changes so they are retained after a reboot:

```
(host) [mynode] #write memory
```

The following example deletes the running configuration and returns controller to the factory default settings:

```
(host) [mynode] #write erase
```

Command History

Release	Modification
ArubaOS 8.11.0.0	The write erase and write erase all commands can be issued only from the /mm and /mm/mynode nodes of the controller.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on acontroller.

zeroize-tpm-keys

zeroize-tpm-keys

Description

This command is used to erase the TPM content and render a controller permanently inoperable.



This command can be issued only on a controller which is runs a FIPS build.

Example

Execute the following command to erase the TPM content and render a controller permanently inoperable.

```
(host) [mynode] (config) #zeroize-tpm-keys
The effect of the action you are about to execute is not reversible. Are you
sure you want to implement this function? Press 'y' to proceed : [y/n]: y
This action will void the warranty on the controller and nullify the RMA.
Are you still sure you want to do this?(y/n): y
You are about to wipe the contents of the TPM and render the controller
permanently inoperable. Are you ready to go ahead?(y/n): y
TPM keys have been zeroized. Please reload the controller.
```

Command History

Release	Modification
ArubaOS 8.4.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable Mode.

zigbee service-profile

```
zigbee service-profile <service-profile>
  clone <source>
  no
  panid <panid>
  permit-joining {off|on}
  radio-instance {all|external|internal}
  security {disable|enable}
  trust-center-link-key <trust-center-link-key>
```

Description

This command configures or modifies a ZigBee service profile.

Parameter	Description
clone	Copy ZigBee service profile data from another ZigBee service profile.
no	Removes any existing configuration.
panid	ZigBee hexadecimal Pan identity. auto, 0000-FFF0
permit-joining	Allow or disallow joining. off, on
radio-instance	The IoT ZigBee radio instance. all, external, internal
security	Enable or disable ZigBee security. disable, enable
trust-center-link-key <trust-center-link-key>	Zigbee trust center link key consisting of 16 hexadecimal bytes.

Example

The following example configures a ZigBee service profile:

```
(host) [mynode] (config) #zigbee service-profile sample_zb_service_profile
(host) [mynode] (ZigBee Service Profile "sample_zb_service_profile") #panid
auto
(host) [mynode] (ZigBee Service Profile "sample_zb_service_profile")
#permit-joining on
```

```
(host) [mynode] (ZigBee Service Profile "sample_zb_service_profile") #radio-  
instance all  
(host) [mynode] (ZigBee Service Profile "sample_zb_service_profile")  
#security enable
```

Related Commands

Command	Description
show zigbee service-profile	Shows the ZigBee service profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

zigbee socket-device-profile

```
zigbee socket-device-profile <profile-name>
  clone <source>
  inbound <inbound>
  no
  outbound <inbound>
```

Description

This command configures or modifies a ZigBee socket device profile.

Parameter	Description
clone	Copy ZigBee socket device profile data from another ZigBee socket device profile.
inbound <inbound>	Inbound socket from ZigBee inbound socket profile.
no	Server URL for authentication.
outbound <outbound>	Outbound socket from ZigBee outbound socket profile.

Example

```
The following example configures a ZigBee socket device profile:
(host) [mynode] (config) #zigbee socket-device-profile sample_zb_socket_
device_profile
(host) [mynode] (Zigbee Socket Device Profile "sample_zb_socket_device_
profile") #inbound sample_zb_socket_inbound_profile
(host) [mynode] (Zigbee Socket Device Profile "sample_zb_socket_device_
profile") #outbound sample_zb_socket_outbound_profile
```

Related Commands

Command	Description
show zigbee socket-device-profile	Shows the ZigBee socket device profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

zigbee socket-inbound-profile

```
zigbee socket-inbound-profile <profile-name>
  clone <source>
  cluster <cluster>
  endpoint <endpoint>
  no
  profile <profile>
  source-endpoint <source-endpoint>
```

Description

This command configures or modifies a ZigBee socket inbound profile.

Parameter	Description
clone <source>	Copy ZigBee socket inbound profile data from another ZigBee socket inbound profile.
cluster <cluster>	The cluster identity. 0x0000 to 0x7FFF and 0xFC00 to 0xFFFF
endpoint <endpoint>	The destination endpoint. 1 to 254
no	Removes any existing configuration.
profile <profile>	The profile identity. 0x0000 to 0x7FFF and 0xC000 to 0xFFF
source-endpoint <source-endpoint>	The source endpoint. 1 to 254

Example

The following example configures a ZigBee socket inbound profile:

```
(host) [mynode] (config) #zigbee socket-inbound-profile sample_zb_socket_inbound_profile
(host) [mynode] (Zigbee Socket Inbound Profile "sample_zb_socket_inbound_profile") #cluster 0x1234
(host) [mynode] (Zigbee Socket Inbound Profile "sample_zb_socket_inbound_profile") #endpoint 12
(host) [mynode] (Zigbee Socket Inbound Profile "sample_zb_socket_inbound_profile") #profile 34
(host) [mynode] (Zigbee Socket Inbound Profile "sample_zb_socket_inbound_profile") #source-endpoint 56
```

Related Commands

Command	Description
show zigbee socket-inbound-profile	Shows the ZigBee socket inbound profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

zigbee socket-outbound-profile

```
zigbee socket-outbound-profile <profile-name>
  asp-ack
  clone
  cluster
  endpoint
  no
  profile
  source-endpoint
```

Description

This command configures or modifies a ZigBee socket outbound profile.

Parameter	Description
asp-ack	Enables acknowledge of AP.
clone <source>	Copy ZigBee socket outbound profile data from another ZigBee socket outbound profile.
cluster <cluster>	The cluster identity. 0x0000 to 0x7FFF and 0xFC00 to 0xFFFF
endpoint <endpoint>	The destination endpoint. 1 to 254
no	This ID identifies the sender to the server.
profile <profile>	The profile identity. 0x0000 to 0x7FFF and 0xC000 to 0xFFF
source-endpoint <source-endpoint>	The source endpoint. 1 to 254

Example

The following example configures a ZigBee socket outbound profile:

```
(host) [mynode] (config) #zigbee socket-outbound-profile sample_zb_socket_
outbound_profile
(host) [mynode] (Zigbee Socket Outbound Profile "sample") #aps-ack
(host) [mynode] (Zigbee Socket Outbound Profile "sample_zb_socket_outbound_
profile") #cluster 0x1234
(host) [mynode] (Zigbee Socket Outbound Profile "sample_zb_socket_outbound_
profile") #endpoint 12
```



```
(host) [mynode] (Zigbee Socket Outbound Profile "sample_zb_socket_outbound_profile") #profile 34
(host) [mynode] (Zigbee Socket Outbound Profile "sample_zb_socket_outbound_profile") #source-endpoint 56
```

Related Commands

Command	Description
show zigbee socket-outbound-profile	Shows the ZigBee socket outbound profile.

Command History

Release	Modification
ArubaOS 8.7.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration IoT Data Profile Mode (config-submode).

What's New in ArubaOS 8.11.1.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.11.1.0.

New Commands in ArubaOS 8.11.1.0

There are no new commands introduced in this release.

Modified Commands in ArubaOS 8.11.0.0

The following commands were modified in ArubaOS 8.11.0.0.

Command	Description
show ap monitor ap-list	The verbose sub-parameter is added to the show ap monitor ap-list ap-name <ap-name> command .
dump-collection-profile	The dump-auto-uploading-profile parameter is introduced.

What's New in ArubaOS 8.11.0.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.11.0.0.

New Commands in ArubaOS 8.11.0.0

The following commands were introduced in ArubaOS 8.11.0.0.

Command	Description
ap remote-debug-pkt	This command enables the packet debugging functionality to troubleshoot data packets handled by the AP.
show airgroup query-result	This command displays the list of AirGroup servers that are available for a client.
show ap cellular bearer	This command displays the dual access point name (APN) details on the SIM of an Aruba USB LTE modem.
show ap remote-debug-pkt	This command displays the packet debugging details of an AP.

Modified Commands in ArubaOS 8.11.0.0

The following commands were modified in ArubaOS 8.11.0.0.

Command	Description
aaa authentication via global-config	The max-via-vpn-sessions parameter is introduced.
airgroupprofile	The include-domain-name parameter is introduced.
airgroup	The send-query parameter is introduced.
show airgroup status	The command output is modified to include the Include domain for username policy parameter
show ap bss-table	The command output is modified to include the following flags: z = WPA3-AES-CCM128 BSS Z = WPA3-AES-CCM128 BSS with transition mode
ap regulatory-domain-profile	The oob_switch parameter is introduced.
ap system-profile	<p>The following modifications are introduced:</p> <ul style="list-style-type: none"> ■ The following changes are made to the ipm-power-reduction-step-prio ipm-step parameter: <ul style="list-style-type: none"> ● Replaced radio_2ghz_chain_1x1 with radio_1_chain_1x1 ● Replaced radio_2ghz_chain_2x2 with radio_1_chain_2x2 ● Replaced radio_2ghz_chain_3x3 with radio_1_chain_3x3 ● Replaced radio_2ghz_disable with radio_1_disable ● Replaced radio_2ghz_power_3dB with radio_1_power_3dB ● Replaced radio_2ghz_power_6dB with radio_1_power_6dB ● Replaced radio_5ghz_2_chain_1x1 with radio_2_chain_1x1 ● Replaced radio_5ghz_2_chain_2x2 with radio_2_chain_2x2 ● Replaced radio_5ghz_2_chain_3x3 with radio_2_chain_3x3 ● Replaced radio_5ghz_2_disable with radio_2_disable ● Replaced radio_5ghz_2_power_3dB with radio_2_power_3db ● Replaced radio_5ghz_2_power_6dB with radio_2_power_6db ● Replaced radio_5ghz_chain_1x1 with radio_0_chain_1x1 ● Replaced radio_5ghz_chain_2x2 with radio_0_chain_2x2 ● Replaced radio_5ghz_chain_3x3 with radio_0_chain_3x3 ● Replaced radio_5ghz_chain_4x4 with radio_0_chain_4x4 ● Replaced radio_5ghz_chain_5x5 with radio_0_chain_5x5 ● Replaced radio_5ghz_chain_6x6 with radio_0_chain_6x6 ● Replaced radio_5ghz_chain_7x7 with radio_0_chain_7x7 ● Replaced radio_5ghz_disable with radio_0_disable

Command	Description
	<ul style="list-style-type: none"> ● Replaced radio_5ghz_power_3dB with radio_0_power_3dB ● Replaced radio_5ghz_power_6dB with radio_0_power_6dB ● Replaced radio_6ghz_chain_1x1 with radio_2_chain_1x1 ● Replaced radio_6ghz_chain_2x2 with radio_2_chain_2x2 ● Replaced radio_6ghz_chain_3x3 with radio_2_chain_3x3 ● Replaced radio_6ghz_disable with radio_2_disable ● Replaced radio_6ghz_power_3dB with radio_2_power_3dB ● Replaced radio_6ghz_power_6dB with radio_2_power_6dB ■ The flex-radio-mode {2.4GHz 2.4GHz-and-5GHz 5GHz} parameter is removed for stand-alone controllers only (ArubaOS 8.11.0.0 or later versions).
ap system-profile	The flex-dual {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz} and flex-dual-mode {2.4GHz-and-6GHz 5GHz-and-2.4GHz 5GHz-and-6GHz Automatic} parameters are introduced to configure flex dual band on AP-615.
clear	The clear lc-cluster bucketmap publish counters command is added to clear the bucketmap publish counters on the cluster.
configure terminal	The ids unauthorized-device-profile parameter is introduced. It includes the following sub-parameters: <ul style="list-style-type: none"> ■ detect-wifi-direct-p2p-groups ■ wifi-direct-network-quiet-time ■ protect-wifi-direct-p2p-groups
crypto-local ipsec-map	The command output of the ipsec-mtu <mtu> parameter is modified to display the MTU size upto 9216 bytes when Jumbo frames are enabled in an IPsec site-to-site tunnel between two managed devices.
firewall	The default value for attack-rate arp parameter is now set to 100.
halt	The halt command can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.
iot transportProfile	The blePeriodicTelemetryDisable parameter is introduced to disable periodic telemetry reporting.
ids unauthorized-device-profile	The vendor-specific-ie-exclusion parameter is introduced.
ip default-gateway	Starting from ArubaOS 8.11.0.0, you can execute the ip default-gateway mgmt <nexthop> CLI command to configure the default gateway on the OOB management port for 7000 Seriescontrollers.
reload	The reload command can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.

Command	Description
rf dot11-6ghz-radio-profile	The frame-bursting-mode and rts-mode parameters are introduced.
rf dot11a-radio-profile	The frame-bursting-mode and rts-mode parameters are introduced.
rf dot11a-secondary-radio-profile	The frame-bursting-mode and rts-mode parameters are introduced.
rf dot11g-radio-profile	The frame-bursting-mode and rts-mode parameters are introduced.
show aaa authentication via global-config	The command output is modified to display the maximum number of concurrent VIA VPN sessions allowed per user.
show aaa state debug-statistics	The command output is modified to display the number of VIA VPN sessions initiated beyond the assigned limit.
show airgroup cppm	The flag, D is introduced in the output of the command to indicate that the servers share the same username.
show airgroup servers	The following modifications are introduced: <ul style="list-style-type: none"> ■ The username parameter is introduced. ■ The flag, D is introduced in the output of the command to indicate that the servers share the same username.
show ap active	New flags, x , y , and z are introduced to indicate the flex dual band support for the AP-615.
show ap database	All available flags are included in the flags <flags> sub-parameter.
show ap monitor ap-list	The following modifications are introduced: <ul style="list-style-type: none"> ■ The wifi-direct [all] parameter is introduced to the show ap monitor ap-list ap-name <ap name> command, which lists all the WIFI-Direct devices detected by the specified AP. ■ The containment-exclusion parameter is introduced to the show ap monitor ap-list ap-name <ap name> command to display the details of containment exclusion.
show ap monitor debug	The following modifications are introduced: <ul style="list-style-type: none"> ■ The show ap monitor debug status ap-name <ap-name> command includes new counters that show detected and discarded Apple Wireless Direct Link frames. ■ The output of the show ap monitor debug profile-config command includes the details of containment exclusion.
show ap regulatory-domain-profile	The command output is modified to display OOB 6GHz scanning for AP-615 settings.
show crypto-local ipsec-map	The command output of the ipsec-mtu <mtu> parameter is modified to display the MTU size upto 9216 bytes when Jumbo frames are enabled in an IPsec site-to-site tunnel between two managed devices.
show crypto isakmp	The command output is modified to display the number of VIA VPN sessions initiated beyond the assigned limit.

Command	Description
show datapath	The supported range for the MTU parameter in the show datapath tunnel command is increased to 9216 bytes when Jumbo frames are enabled in an IPsec site-to-site tunnel between two managed devices.
show ip route	The command output was modified to display the configured default gateway on the OOB management port for 7000 Series controllers.
show lc-cluster	The bucket distribution all , bucket distribution essid <ssid-name> , and bucketmap publish counters parameters are added to display the bucketmap distribution for the cluster.
show rf dot11a-radio-profile	The command output is modified to display the status of Frame Bursting Mode and RTS Mode .
show rf dot11a-secondary-radio-profile	The command output is modified to display the status of Frame Bursting Mode and RTS Mode .
show rf dot11g-radio-profile	The command output is modified to display the status of RTS Mode .
show rf dot11-6GHz-radio-profile	The command output is modified to display the status of Frame Bursting Mode and RTS Mode .
show snmp trap-list	The command output is modified to display the new SNMP trap, wlsxLicenseThresholdLimitHit , when the license usage is more than 75% of the allocated licenses and before all licenses are used. By default, this SNMP trap is disabled.
show snmp trap-queue	The command output is modified to display the new SNMP trap, wlsxLicenseThresholdLimitHit , when the license usage is more than 75% of the allocated licenses and before all licenses are used. By default, this SNMP trap is disabled.
show web-server	The command output is modified to display the list of enabled cipher suites for the controller.
snmp-server	A new SNMP trap, wlsxLicenseThresholdLimitHit , is introduced to send an alert when the license usage is more than 75% of the allocated licenses and before all licenses are used. By default, this SNMP trap is disabled.
web-server profile	The cipher-suite <cipher(s)> parameter is introduced. The ciphers parameter is removed.
write	The write erase and write erase all commands can be issued only from the /mm and /mm/mynode nodes of the Mobility Conductor.

Deprecated Commands in ArubaOS 8.11.0.0

The following commands were deprecated in ArubaOS 8.11.0.0.

Command	Description
<pre> lc-cluster group-profile <profile> active-ap-lb active-ap-rebalance-ap-count <active-ap-rebalance-ap-count> active-ap-rebalance-threshold-percentage <active-ap-rebalance-threshold- percentage> active-ap-rebalance-timer <active-ap-rebalance-timer> active-ap-unbalance-threshold-percentage <active-ap-unbalance-threshold- percentage> clone <source> controller <ip> [priority <prio>] [mcast-vlan <mcast_vlan>] [vrrp-ip <vrrp_ip> vrrp-vlan <vrrp_vlan> group <group number>] controller-v6 <ipv6> heartbeat-threshold <heartbeat-threshold> redundancy rapcluster vrrp-id <starting id> </pre>	<p>The active-client-rebalance-threshold, standby-client-rebalance-threshold, and unbalance-threshold parameters are removed.</p>
<pre> ap wifi-uplink-profile opmode {static-wep} wepkey1 <wepkey1> wepkey2 <wepkey2> wepkey3 <wepkey3> wepkey4 <wepkey4> weptxkey <weptxkey> </pre>	<p>The following parameters configured the WEP settings for Wi-Fi uplink profile:</p> <ul style="list-style-type: none"> ■ <code>static-wep</code> with static keys. ■ <code>wepkey1 <wepkey1></code>—The first static WEP

Command	Description
	<p>key associated with the key index.</p> <ul style="list-style-type: none"> ■ <code>wepkey2 <wepkey2></code>—The second static WEP key associated with the key index. ■ <code>wepkey3 <wepkey3></code>—The third static WEP key associated with the key index. ■ <code>wepkey4 <wepkey4></code>—The fourth static WEP key associa

Command	Description
	<p>ted with the key index.</p> <ul style="list-style-type: none"> ▪ weptx key <wept xkey> <p>—The key index to specify which static WEP key was to be used.</p>

What's New in ArubaOS 8.10.0.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.10.0.0.

New Commands in ArubaOS 8.10.0.0

The following commands were introduced in ArubaOS 8.10.0.0:

Command	Description
ap modem-upgrade	This command configures the firmware upgrade of Aruba USB LTE modem.
ap modem	This command upgrades the firmware version of Aruba AP USB LTE modem from the managed device.
gps	This command configures the GPS profile.
show ap cellular connection-lte-logs	This command displays the LTE connection logs for a USB modem connected to an AP.
show ap cellular operator	This command displays the network operator information.
show ap cellular signal	This command displays the signal information for a USB modem connected to an AP.

Command	Description
<u>show ap cellular sim</u>	This command displays information on the SIM card of a USB modem connected to an AP.
<u>show ap cellular stats</u>	This command displays statistics on the transmitted and received data bytes of a USB modem connected to an AP.
<u>show ap cellular status</u>	This command displays the overall status of Aruba USB modem.
<u>show ap cellular cell</u>	This command displays the network cell information for an AP connected to modem.
<u>show ap cellular connection-logs</u>	This command displays the connection logs for a USB modem connected to an AP.
<u>show ap cellular</u>	This command displays the cellular information for debugging purposes.
<u>show ap debug client-kickout-logs</u>	This command displays detailed information on last 12 occurrences of the client kickout (deauthentication) logs per radio in 530 Series, 550 Series, 630 Series, and 650 Series access points.
<u>show ap gps</u>	This command displays the status of GPS profile.
<u>show ap modem-download-log</u>	This command displays the download logs of Aruba USB LTE modem firmware.
<u>show ap modem-upgrade-status</u>	This command displays the status of Aruba USB LTE modem firmware upgrade.
<u>show ap usb verbose</u>	This command displays the details of Aruba USB modem.
<u>show tm</u>	This command displays the monitoring update queue information of the telemetry manager module.
<u>tm</u>	This command is used to configure the maximum queue size for the TM monitoring updates.

Modified Commands in ArubaOS 8.10.0.0

The following commands were modified in ArubaOS 8.10.0.0:

Command	Description
<u>aaa authentication-server radius</u>	The range of the RADIUS server authentication timeout value is increased from 1-30 seconds to 1-120 seconds.
<u>aaa password-policy mgmt</u>	The range of characters in the management user password is increased from 6-64 to 6-128.
<u>ap system-profile</u>	The sub-parameter transfer-enable was added to the dump-collection-profile parameter.

Command	Description
ap system-profile	The following sub-parameters are added to the ipm-power-reduction-step-prio ipm-step parameter: <ul style="list-style-type: none"> ▪ radio_2ghz_disable ▪ radio_5ghz_disable ▪ radio_5ghz_2_chain_1x1 ▪ radio_5ghz_2_chain_2x2 ▪ radio_5ghz_2_chain_3x3 ▪ radio_5ghz_2_disable ▪ radio_5ghz_2_power_3dB ▪ radio_5ghz_2_power_6dB ▪ radio_6ghz_chain_1x1 ▪ radio_6ghz_chain_2x2 ▪ radio_6ghz_chain_3x3 ▪ radio_6ghz_disable ▪ radio_6ghz_power_3dB ▪ radio_6ghz_power_6dB
crypto ipsec	The maximum transmission unit (MTU) range for the <code><max_mtu></code> parameter is increased from 1024-1500 to 1024-2500. This is supported in IPsec site-to-site tunnels for the virtual mobility controllers (VMC)s.
firewall-visibility	The feed <sort-by-bssid> parameter is introduced.
ids dos-profile	The following ghost tunnel attack detection parameters are added: <ul style="list-style-type: none"> ▪ detect-ghosttunnel-client-attack ▪ detect-ghosttunnel-server-attack ▪ ghosttunnel-client-attack-interval ▪ ghosttunnel-client-attack-threshold ▪ ghosttunnel-client-quiet-time ▪ ghosttunnel-server-attack-interval ▪ ghosttunnel-server-attack-threshold ▪ ghosttunnel-server-quiet-time
ip default-gateway	The ip default-gateway mgmt <nexthop> command was modified to configure the default gateway for dedicated OOB management Ethernet port on 7000 Series controllers.
mgmt-user	The management username can have a maximum of 128 characters.
provision-ap	The following parameters are introduced: <ul style="list-style-type: none"> ▪ aruba-modem-apn <aruba-modem-apn> ▪ aruba-modem-plmn <aruba-modem-plmn>
rf dot11g-radio-profile	The airmatch-mode-aware parameter was introduced to enable or disable the AirMatch mode aware.
show ap active type	The airmatch-monitor parameter was introduced to show information of AirMatch monitors.

Command	Description
show ap arm client-match summary	The output of the show ap arm client-match summary and show ap arm client-match summary advanced commands is modified to include the following fields for Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ B5G (T/S) ■ B6G (T/S)
show ap arm client-match unsupported	The command output is modified to include the following flags for Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ B5G ■ B6G
show ap debug airmatch	The output of the command was modified to include the Probe Type parameter under the AirMatch Reporting Radio Band 2.4GHz table.
show ap debug power-table	The command output is modified to include Flash EIRP Limit parameter for 6 GHz bands.
show ap monitor debug	The probe type airmatch-am is introduced in the output of the command under WLAN Interface table.
show ap wifi-uplink-profile	The command output is modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ 6GHz value for Allowed band parameter. ■ WPA3-SAE-AES value for Encryption parameter.
show ap wifi-uplink candidates	The command output is modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ 6GHz value for band parameter. ■ WPA3 value for encryption parameter.
show ap wifi-uplink connection-history	The command output is modified to display 6GHz value for band parameter on Wi-Fi 6E APs.
show ap wifi-uplink neighbors	The command output is modified to display the following changes on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ 6GHz value for band parameter. ■ WPA3 value for encryption parameter.
show ap wifi-uplink status	The command output is modified to display the following parameter values on Wi-Fi 6E APs: <ul style="list-style-type: none"> ■ wpa3-sae-aes value for Unicast/Multicast Encryption parameter. ■ 6GHz value for Phy parameter.
show crypto-local ipsec-map	Displays PPK ID in the IPsec map configurations on a controller.
show crypto-local isakmp	The ppk parameter was introduced.
show crypto isakmp	The output of the command was modified to display the PPK exchange value.
show firewall-visibility	The show firewall-visibility status command output is modified to include the Sort by Bssid Status parameter.
show ids dos-profile	The following ghost tunnel attack detection parameters are added:

Command	Description
	<ul style="list-style-type: none"> ▪ Detect GHOST TUNNEL SERVER Attack ▪ Detect GHOST TUNNEL CLIENT Attack ▪ GHOST TUNNEL Attack Beacon Detection Threshold ▪ GHOST TUNNEL Attack Probe Request Detection Threshold ▪ GHOST TUNNEL Attack Detection Time Interval ▪ GHOST TUNNEL Attack Detection Time Interval ▪ Ghosttunnel Attack Detection SERVER Quiet Time ▪ Ghosttunnel Attack Detection CLIENT Quiet Time
show interface gigabitethernet	A new output parameter Aruba Certified was introduced.
show memory	The tm parameter is introduced.
show mgmt-server	The tm process is introduced.
	The range of characters in the management username is increased from 1-64 to 1-128.
show mon-serv-mesh-tbl-entry	The 6G parameter is introduced.
show rf dot11g-radio-profile	The output of the show rf dot11g-radio profile command displays the status of AirMatch Mode Aware .
show stm	The mon-update-queue {stats threshold} parameter is deprecated.
stm	The mon-update-queue <threshold> parameter is deprecated.
wlan dot11k-profile	The nb-resp-wide-band-ie is added to include the wide channel bandwidth information element in the neighbor report responses.

Deprecated Commands in ArubaOS 8.10.0.0

The following commands were deprecated in ArubaOS 8.10.0.0:

Command	Description
<code>airgroup active-domain</code>	This parameter configured active domain for an AirGroup cluster.
<pre>airgroup cppm-server aaa rfc-3576-server <rfc3576_server> rfc3576_udp_port <rfc3576_udp_port> server-dead-time <server-dead-time> server-group <server-group> query-interval <1..24></pre>	<p>This parameter configured the following in an AirGroup AAA profile:</p> <p>rfc-3576-server <rfc3576_server>: Configured the RFC 3576 server IP address.</p> <p>rfc3576_udp_port <rfc3576_udp_port>: Configured the UDP port number.</p> <p>server-dead-time <server-deadtime>: Configured server dead time in minutes.</p> <p>server-group<server-group>: Configured the name of the server group.</p>
<pre>domain <string> description <description></pre>	This parameter configured AirGroup domain.

Command	Description
<pre>ip-address <ipaddr> no</pre>	
<pre>show airgroup cppm-server aaa</pre>	<p>This parameter displayed the ClearPass Policy Manager server details.</p> <ul style="list-style-type: none"> ▪ aaa: Displayed the AAA parameters for AirGroup.
<pre>show airgroup effective profiles</pre>	<p>This parameter displayed the effective profiles that were applied at that node.</p>
<pre>policy-entries mac neighborhood <mac> <mac></pre>	<p>This parameter displayed the active policies.</p> <ul style="list-style-type: none"> ▪ neighborhood - Displayed the AP neighborhood to discover the server. ▪ mac - Displayed active policies filtered by specified MAC address.

What's New in ArubaOS 8.9.0.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.9.0.0.

New Commands in ArubaOS 8.9.0.0

The following commands were introduced in ArubaOS 8.9.0.0:

Command	Description
rf dot11-6ghz-radio-profile	This command configures Wi-Fi 6E AP radio settings for the 6 GHz frequency band on a 802.11 6 GHz radio profile, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.
show ap active 6GHz	This command displays information related to 6 GHz radio that is active on Wi-Fi 6E APs.
wlan 6ghz-rrm-ie-profile	This command configures a Radio Resource Management (RRM) Information Elements (IE) profile to define the information elements advertised by a Wi-Fi 6E AP for 6 GHz band.

Modified Commands in ArubaOS 8.9.0.0

The following commands were modified in ArubaOS 8.9.0.0:

Command	Description
ap mesh-radio-profile	The 6 GHz sub-parameter under prefer-uplink-radio parameter was introduced for Wi-Fi 6E APs.
ap regulatory-domain-profile	The following parameters were introduced for Wi-Fi 6E APs:

Command	Description
	<ul style="list-style-type: none"> ▪ utb_filter_block ▪ valid-6ghz-channel <valid-6ghz-channel>
ids general-profile	The wireless-containment-death-reason parameter was introduced.
iot transportProfile	<p>The following parameters were introduced:</p> <ul style="list-style-type: none"> ▪ usbSerialDeviceTypeFilter <filter> ▪ companyIdentifierFilter <filter> ▪ serviceUUIDFilter <filter> ▪ macOuiFilter <filter> ▪ localNameFilter <filter>
logging	The tls sub-parameter was introduced to ensure secure transport mechanism to send device logs to an external logging server.
rf arm-profile	The default-6ghz parameter was introduced.
show ap active	The 6GHz parameter was introduced for Wi-Fi 6E APs.
show ap allowed-channels	<p>The command output was modified to include the following:</p> <ul style="list-style-type: none"> ▪ Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values respectively under PHY Type parameter ▪ Added 6GHz value under PHY Type parameter for Wi-Fi 6E APs.
show ap arm history	The Phy-Type parameter was introduced.
show ap arm neighbors	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> ▪ Added phy-type parameter. ▪ Added 2.4GHz, 5GHz, and 6GHz values for phy-type parameter.
show ap arm rf-summary	<p>The command output was modified to include the following parameters:</p> <ul style="list-style-type: none"> ▪ band ▪ phy-type
show ap arm scan-times	<p>The command output was modified to include following parameters:</p> <ul style="list-style-type: none"> ▪ band

Command	Description
	<p>The command output was modified to include the UTB filter results, and based on the band selected the following parameters were displayed:</p> <ul style="list-style-type: none"> ▪ First blocked channel ▪ Last blocked channel
show ap association	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ▪ Added 2, 5, and 6 values to denote 2.4 GHz, 5 GHz, and 6 GHz bands respectively for the phy <phy> parameter. ▪ Added 2.4GHz, 5GHz, and 6GHz values for phy and phy_cap output parameters.
show ap bss-table	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> ▪ Replaced 802.11g and 802.11a with 2.4GHz and 5GHz parameters respectively. ▪ Added 6Ghz parameter for Wi-Fi 6E APs.
show ap config	<p>The command output was modified to display the 2.4GHz, 5GHz, 5GHz-secondary, and 6GHz parameters.</p>
show ap debug airmatch	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ▪ The Radio 2 interface was displayed for 6 GHz band on Wi-Fi 6E APs. ▪ The command outputs were modified to include 6 GHz values for Wi-Fi 6E APs. ▪ The show ap debug airmatch channel-lists ap-name <ap-name> command output was modified to include u channel flag and 6 GHz data for Wi-Fi 6E APs.
show ap debug bss-config	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ▪ Replaced phy with band/ht-mode/bandwidth parameter in the command output. ▪ Replaced g and a with 2.4GHz and 5GHz values in the command output. ▪ Added 6GHz value in the command output for Wi-Fi 6E APs. ▪ Added x flag in the command output parameter for Wi-Fi 6E APs.

Command	Description
show ap debug received-reg-table	The 6g value was introduced under PHY Type output parameter for Wi-Fi 6E APs.
show ap essid	The command output was modified to include the MBSSID Tx BSS parameter for Wi-Fi 6E APs.
show ap-group	The command output was modified to display the 802.11 6GHz radio profile parameter.
show ap load-balancing	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Replaced phy with Phy-type parameter. ▪ Replaced a and g with 5GHz and 2.4GHz values. ▪ Introduced 6GHz value for Wi-Fi 6E APs.
show ap mesh active	The command output was modified to display the RF bands as 2.4 GHz , 5 GHz , or 6 GHz .
show ap mesh neighbors	The following changes were made: <ul style="list-style-type: none"> ▪ All instances of Blacklisted-neighbour have been replaced with Denylisted-neighbour. ▪ The output of the command was modified to display the AP Name and Band parameters.
show ap monitor active-laser-beams	The 6GHz value was added to band <band> parameter for Wi-Fi 6E APs.
show ap monitor ap-list	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Removed chan and phy-type parameters. ▪ Added band/chan/ch-width/ht-type and 6Ghz capable parameters for Wi-Fi 6E APs.
show ap monitor association	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Replaced phy-type with band ▪ Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for band output parameter respectively. ▪ Introduced 6GHz value under band parameter for Wi-Fi 6E APs.

Command	Description
show ap monitor client-list	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced phy-type with band/chan/ch-width/ht-type parameter. Introduced 6GHz capable parameter for Wi-Fi 6E APs.
show ap monitor debug	<p>The output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced phy-type with band/chan/ch-width/ht-type. Replaced 802.11g and 802.11a with 2.4GHz and 5GHz. Introduced 6GHz parameter for Wi-Fi 6E APs.
show ap monitor mesh-list	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced phy-type with band/chan/ch-width/ht-type parameter. Introduced 6GHz capable parameter for Wi-Fi 6E APs.
show ap monitor pot-ap-list	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced channel and phy with band/chan parameter. Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for band/chan output parameter respectively. Introduced 6GHz value under band/chan parameter for Wi-Fi 6E APs.
show ap monitor pot-client-list	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced channel with band/chan parameter. Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for band output parameter respectively. Introduced 6GHz value under band/chan parameter for Wi-Fi 6E APs.
show ap monitor scan-info	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced 802.11g and 802.11a with 2.4GHz and 5GHz values for Phy

Command	Description
	<p>Type output parameter respectively.</p> <ul style="list-style-type: none"> Introduced 6GHz value under Phy Type parameter for Wi-Fi 6E APs.
<p>show ap radio-database</p>	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced band [a g] with band [2.4GHz 5GHz 6GHz] parameters. Replaced Radio 0 Band Ch/EIRP/MaxEIRP/Clients with Radio 0 Band/Chan/HT-Type/EIRP in the output parameter. Replaced Radio 1 Band Ch/EIRP/MaxEIRP/Clients with Radio 1 Band/Chan/HT-Type/EIRP in the output parameter. Replaced Radio 2 Band Ch/EIRP/MaxEIRP/Clients with Radio 2 Band/Chan/HT-Type/EIRP in the output parameter.
<p>show ap radio-summary</p>	<p>The command was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced dot11a and dot11g with 5GHz and 2.4GHz parameters respectively. Introduced 6GHz parameter for Wi-Fi 6E APs. Introduced 6GHz value under Band output parameter for Wi-Fi 6E APs.
<p>show ap regulatory-domain-profile</p>	<p>The command output was modified to display the following new parameters for Wi-Fi 6E APs:</p> <ul style="list-style-type: none"> UTB Filter Blocking Selection Valid 6GHz channel Valid 6GHz 40MHz channel pair Valid 6GHz 80MHz channel group Valid 6GHz 160MHz channel group
<p>show ap remote bss-table</p>	<p>The command output was modified to include the following changes:</p> <ul style="list-style-type: none"> Replaced phy parameter with band/ht-mode/bandwidth. Added x and 3 flags.
<p>show ap remote debug association</p>	<p>The command output was modified to display the following values for phy parameter:</p> <ul style="list-style-type: none"> 2.4GHz

Command	Description
	<ul style="list-style-type: none"> ▪ 5GHz ▪ 6GHz (For Wi-Fi 6E APs)
show ap remote debug bss-config	<p>The command output was modified to include the following:</p> <ul style="list-style-type: none"> ▪ Replaced phy parameter with band/ht-mode/bandwidth. ▪ Added x and 3 flags.
show ap remote debug neighbor-cache	<p>The command output was modified to include the Band parameter.</p>
show ap spectrum channel-metrics	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap spectrum channel-summary	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap spectrum client-list	<p>The following changes were introduced:</p> <ul style="list-style-type: none"> ▪ The band <band> parameter was added. ▪ Replaced phy-type with band in the command output parameter.
show ap spectrum debug status	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap spectrum device-list	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs..</p>
show ap spectrum device-log	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap spectrum device-history	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap spectrum interference-power	<p>Introduced the 6ghz sub-parameter under freq-band parameter for Wi-Fi 6E APs.</p>
show ap snmp	<p>The command output was modified to include 2.4GHz, 5GHz, and 6GHz values for Channel parameter.</p>
show ap virtual-beacon-report	<p>The 6 GHz capable parameter was introduced.</p>
show ap wmm-flow	<p>The following parameters were introduced:</p>

Command	Description
	<ul style="list-style-type: none"> ▪ 2.4GHz ▪ 5GHz ▪ 6GHz (For Wi-Fi 6E APs)
<u>show ids general-profile</u>	The wireless-containment-deauth-reason parameter was introduced. .
<u>show ip route</u>	The command output was modified to display the configured default gateway on the OOB management port for 7280 controllers.
<u>show wms ap</u>	The following changes were introduced: <ul style="list-style-type: none"> ▪ Introduced Band parameter in the output of the show wms ap list and show wms ap tree commands. ▪ Introduced 2.4GHz, 5GHz, and 6GHz values under Band parameter.
<u>show wms client</u>	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Introduced Band parameter in the output of show wms client list command. ▪ Introduced Band/Chan/HT-Type/HT-Sec-Chan parameter in the output of show wms client <mac> command. ▪ Introduced 2.4GHz, 5GHz, and 6GHz values under Band parameter.
<u>show wms probe</u>	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Introduced Band/HT-Type parameter. ▪ Introduced 2.4GHz, 5GHz, and 6GHz values under Band parameter.
<u>show wms rogue-ap</u>	The command output was modified to include the following changes: <ul style="list-style-type: none"> ▪ Introduced Band parameter under show wms rogue-ap list command. ▪ Introduced 2.4GHz, 5GHz, and 6GHz values under Band parameter. ▪ Introduced Band/Chan/HT-Type/HT-Sec-Chan parameter under show wms rogue-ap <bssid> command.
<u>show logging</u>	The output sub-parameter tls was introduced.

Command	Description
show running-config	The command output was modified to display the configured default gateway on the OOB management port for 7280 controllers.
wlan dot11k-profile	The ap-chan-rpt-6ghz parameter was introduced.
wlan bcn-rpt-req-profile	The values auto , 81 , 115 , and 131 were introduced for the reg-class parameter.
wlan virtual-ap	The following changes were made: <ul style="list-style-type: none"> Introduced allowed-band-6ghz and disable-on-6ghz-mesh parameters. Introduced none option under allowed-band parameter.

What's New in ArubaOS 8.8.0.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.8.0.0.

New Commands in ArubaOS 8.8.0.0

The following commands were introduced in ArubaOS 8.8.0.0:

Command	Description
acl-debug alias-rule-hits type	This command allocates hits-indices for role, route, and session ACEs expanded in an ACE with aliases.
allowed-address-list	This command configures addresses exempted when the deny-inter-user-bridging is enabled.
iot-sniffer radio	This command configures the IoT sniffer function on the radio of an AP.
ip dhcp reserved	This command configures DHCP server device reservations. You can use IP reservation to manually bind IP addresses from a DHCP pool to a client MAC address.
ipv6 dhcp relay-option	This command configures the DHCPv6 relay options by using the XML definition file containing DHCPv6 Option 18 (Circuit ID) and Option 37 (Remote ID) sub-type options.
managed-device delete image	This command deletes the image stored in Mobility Master file system.
no allowed-address-list	This command is used to remove the IP addresses that were added using <code>allowed-address-list</code> command.
show ap antenna status	This command is introduced to display the operational status of AP antennas.
show ap debug iot-sniffer	This command displays IoT sniffer information on the AP.

Command	Description
show ap remote debug web-server-config	This command displays the web server profile configurations on the AP.
show ap remote debug wired-port-down-state	This command displays the wired port bounce configurations that are forwarded from the controller and AP's wired port status.
show managed-device images	This command displays the images of managed devices stored in the Mobility Master file server.
show aaa authentication downloaded-cp-profiles	This command enables users to push CP profiles along with the user role from CPPM.
show snmp trap-group	This command displays the configured SNMP trap groups.

Modified Commands in ArubaOS 8.8.0.0

The following commands were modified in ArubaOS 8.8.0.0:

Command	Description
airgroup	The version parameter was introduced.
ap mesh-radio-profile	The following changes were introduced: <ul style="list-style-type: none"> ■ The optimize-scan-interval parameter was introduced. ■ The functionality of reselect-any-time and subthreshold-only reselection-modes were changed. ■ The mesh-mobility, mobility-beacon-miss <mobility-beacon-miss>, and mobility-rssi <mobility-rssi> parameters are introduced.
ap system-profile	The following parameters are introduced: <ul style="list-style-type: none"> ■ wired-poe-bounce-interval <wired-poe-bounce-interval> ■ wired-port-bounce-interval <wired-port-bounce-interval> ■ seslmagotag-esl-radio-coexistence ■ seslmagotag-esl-tls-auth ■ seslmagotag-esl-tls-fqdn-verify The value, 127, was added to the seslmagotag-esl-channel parameter.
ap provisioning-profile	The following parameters were added: <ul style="list-style-type: none"> ■ apdot1x-timeout-bypass ■ apdot1x-timeout-retries
clear	The ip dhcp binding ip-address <ip-address> parameter is introduced.
crypto-local ipsec-map	The session-acl sub-parameter was added in the ip access-group parameter.
est	The output is modified to specify the keytype in a csr attribute. The default server configuration is accepted first during the enrollment/re-enrollment process. If the server does not provide the csr attribute, then the user configured csr attribute is accepted.

Command	Description
firewall	The session-spread parameter is added.
interface vlan	The ipv6-relay-option parameter is introduced.
iot transportProfile	<p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ■ azure-dps-auth-type group-enrollment symmetric-key ■ azure-dps-id-scope ■ authentication-mode ■ client-secret ■ bleDataForwarding ■ perFrameFiltering <p>The following deviceClassFilters are introduced:</p> <ul style="list-style-type: none"> ■ google ■ minew <p>The Azure-IoTHub server type is introduced.</p>
ip access-list route	The output is modified to display a brief description of the route ACL.
ip access-list session	The output is modified to display a brief description of the session ACL.
ntp	The fqdn sub-parameter is introduced.
provision-ap	<p>The following parameters were added:</p> <ul style="list-style-type: none"> ■ apdot1x-timeout-bypass ■ apdot1x-timeout-retries
rf arm-profile	A new parameter, voip-aware-scan-timer , is added to enable users to set the VoIP Aware Scan Timer range between 50 ms-1000 ms.
rf dot11a-radio-profile	The zero-wait-dfs parameter is introduced.
rf dot11g-radio-profile	The iot-coex-enable parameter is introduced.
show acl acl-table	A new parameter, verbose , shows verbose ACL information.
show airgroup status	A new output parameter, AirGroup version , is introduced to display the active AirGroup version.
show airmatch debug optimization	A new flag, A is introduced to indicate the radios assigned by AirMatch.
show airmatch debug reporting-radio	A new flag, A is introduced to indicate the radios assigned by AirMatch.
show airmatch debug solver feasibility	A new output parameter, HE Pooling Chan Feas is introduced to display the number of HE pooling channels.
show amon-sender	The output parameter, TAG of the show amon-sender stats-counters-all command gets incremented when there are RTLS frames from AMON receiver.
show ap arm scan-times	The output of the command is modified to display the zero-wait DFS channel details.

Command	Description
show ap database	A new flag, b , was introduced to show AP1x timeout.
show ap debug system-status	The following modifications are introduced: <ul style="list-style-type: none"> ■ The output of the command has been modified to display the NSS CPU usage. ■ The output of the command has been modified to display Ethernet related details.
show ap mesh neighbors	The output of the command is modified to display the m flag.
show ap mesh-radio-profile	The output of the command is modified to display the following parameters: <ul style="list-style-type: none"> ■ Mesh Mobility ■ Mobility RSSI Threshold ■ Mobility Beacon Miss Number
show ap monitor debug	The output of the command is modified to display the zero-wait DFS channel details.
show ap system-profile	The output of the command is modified to display the following parameters: <ul style="list-style-type: none"> ■ Wired Port Down-Time By Shutdown Ethernet Link ■ Wired Port Down-Time By Shutdown POE
show ap tech-support	The output of the command is modified to display Ethernet related details.
show crypto-local isakmp	The max-allowed-negotiations parameter was added to show the maximum on-going exchanges allowed at a time.
show datapath	The output of the command is modified to display allowed-address-list .
show firewall	The output of the command is modified to include the DPI classifications.
show gsm debug	The output of the command was modified to include dhcpcd_via_info parameter.
show ip dhcp	The reserved parameter is introduced to display DHCP server device reservations.
show ipv6 dhcp	The following parameters are introduced: <ul style="list-style-type: none"> ■ helper <id> ■ relay <counters> ■ relay-option ■ vlan <id>
show master-l3redundancy/show conductor-l3redundancy	The show master-l3 redundancy switches command now allows users to see the L3 redundant peer controller details along with active and standby controller details.
show snmp trap-list	The output of the command was modified to include a new SNMP trap, wlsxClusterVlanProbeStatus .

Command	Description
show upgrade-profile	The output of the command is modified to display the Download AOS Image from MM parameter.
show wlan he-ssid-profile	The output of the command is modified to include status of uplink MU-MIMO transmission.
show wlan virtual-ap	The output of the command is modified to display the Fine Timing Measurement (802.11mc) Responder Mode parameter.
show wms ap	The output of the show wms ap <bssid> and show wms ap list commands are modified to display the following parameters: <ul style="list-style-type: none"> ■ Match-Type ■ Match-Source ■ Match-Time
snmp-server	The trap-group <SNMP trap group name> parameter is introduced.
upgrade-profile	The download_from_mm parameter is added.
user-role	A new parameter, via-dhcp , is added to support external DHCP server address pool instead of internal L2TP pool
wlan he-ssid-profile	The he-ul-mu-mimo parameter is introduced.
wlan virtual-ap	The ftm-responder-enable parameter is introduced.
user-role	The following parameters were added: <ul style="list-style-type: none"> via-dhcp robust-age-out
wms ap	The <source> sub-parameter is introduced.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.7.0.0.

New Commands in ArubaOS 8.7.0.0

The following commands were introduced in ArubaOS 8.7.0.0:

Command	Description
airslice	This command is introduced to configure or modify an Air Slice profile.
ap debug radio-diag-log	This command is introduced to collect WLAN firmware diagnostic logs to facilitate firmware debugging.
ap get-crash-dumps	This command is introduced to allow AP crash dump files to be transferred to the controller flash memory on demand from the AP flash memory.
ap mesh-accesslist-profile	This command is introduced to configure or modify a mesh access list profile.
ap usb-acl-prof	This command is introduced to configure an AP USB ACL profile.
ap usb-profile	This command is introduced to configure an AP USB profile.
ble service-profile	This command is introduced to configure BLE service profile.
ca-bundle	This command is introduced to upgrade the trusted CA certificates.
dot1x-transactions-monitor	This command is introduced to start or stop displaying the rate statistics under the show dot1x-transactions-monitor command.
dot1x-transactions-monitor set	This command is introduced to provide the rate statistics interval duration and the total duration of a 802.1X transaction.
ip-reputation deny	This command is introduced to deny connections matching malicious IP addresses.
lc-rap-pool-v6	This command is introduced to configure the Remote AP inner IPv6 pool for cluster deployment.
show airslice	This command is introduced to display the details of an Air Slice profile.
show ap debug ble-input-filter-stats	This command is introduced to display the input-filter information in the BLE table.
show ap debug client-info	This command is introduced to display all the details of a specific client in WLAN driver, for client debugging.
show ap debug radio-diag-log status	This command is introduced to display the current diagnostic logging status of an AP.

Command	Description
<u>show ap debug usb-device-mgmt</u>	This command is introduced to display the debugging information of USB devices managed on an AP.
<u>show ap get-crash-dumps-status</u>	This command is introduced to display the status of the crash dump file transfers to a controller.
<u>show ap mesh-accesslist-profile</u>	This command is introduced to display the details of a mesh access list profile.
<u>show ap usb-acl-prof</u>	This command is introduced to display the AP USB ACL profile.
<u>show ap usb-device-mgmt</u>	This command is introduced to display the USB devices managed on an AP.
<u>show ap usb-prof</u>	This command is introduced to display AP USB profile.
<u>show ble service-profile</u>	This command is introduced to display the details of a BLE service profile.
<u>show ca-bundle version</u>	This command is introduced to display the version number of trusted CA certificates.
<u>show dot1x-transactions-monitor</u>	This command is introduced to display the rate statistics, per second, for a 802.1X user.
<u>show datapath cluster details</u>	This command is introduced to display detailed values of heartbeat sent or received count along with the sequence number of missed and delayed packets for all the connected peers.
<u>show datapath cluster heartbeat counters</u>	This command is introduced to display information related to cluster heartbeat counters.
<u>show lc-cluster history</u>	This command is introduced to display the history of the connection and disconnection events with a reason and the time stamp.
<u>show log peer-debug</u>	This command is introduced to display the logs of MAC-based debugging in IKE.
<u>show zigbee service-profile</u>	This command is introduced to display the ZigBee service profile.
<u>show zigbee socket-device-profile</u>	This command is introduced to display the ZigBee socket device profile.
<u>show zigbee socket-inbound-profile</u>	This command is introduced to display the ZigBee socket inbound profile.
<u>show zigbee socket-outbound-profile</u>	This command is introduced to display the ZigBee socket outbound profile.
<u>zigbee service-profile</u>	This command is introduced to configure a ZigBee service profile.
<u>zigbee socket-device-profile</u>	This command is introduced to configure a ZigBee socket device profile.

Command	Description
zigbee socket-inbound-profile	This command is introduced to configure a ZigBee socket inbound profile.
zigbee socket-outbound-profile	This command is introduced to configure a ZigBee socket outbound profile.

Modified Commands in ArubaOS 8.7.0.0

The following commands were modified in ArubaOS 8.7.0.0:

Command	Description
aaa authentication captive-portal	Captive portal authentication was supported for VAPs in the bridge forwarding mode.
aaa authentication via connection-profile	The addr sub-parameter is modified to include IPv6 address.
aaa profile	The ageout-bridge-user parameter is introduced.
airmatch profile	The he-pooling-client-density parameter is introduced.
ap ble-init-action	The following parameters are introduced: <ul style="list-style-type: none"> ▪ input-filter-disable ▪ input-filter-enable
ap-group	The following parameters are introduced: <ul style="list-style-type: none"> ▪ airslice-profile ▪ airslice-visibility record-limit ▪ mesh-accesslist-profile ▪ usb-profile
ap mesh-cluster-profile	The rf-band all and rf-split5G-band-range parameters are introduced.
ap mesh-radio-profile	The prefer-uplink-radio parameter is introduced.
ap-name	The following parameters are introduced: <ul style="list-style-type: none"> ▪ airslice-profile ▪ mesh-accesslist-profile
ap provisioning-profile	The master-preference parameter is introduced.
ap system-profile	The following parameters are introduced: <ul style="list-style-type: none"> ▪ disable-factory-reset ▪ he-pooling-enable ▪ itm-enable The following parameters were modified: <ul style="list-style-type: none"> ▪ telnet

Command	Description
	<ul style="list-style-type: none"> ▪ recovery-mode
controller-ble opmode	The beaconing parameter is removed.
crypto ipsec	The rekey parameter is introduced to configure IPsec rekey interval.
crypto isakmp	The rekey parameter is introduced to configure IKE rekey interval.
firewall	<p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ▪ enable-gre-inner-pkt-frag ▪ deny-needfrag-df-gre-xmit-icmp ▪ deny-needfrag-df-gre ▪ deny-needfrag-gre-xmit-icmp ▪ deny-needfrag-gre
interface vlan	The dns-sl sub-parameter is added.
iot-manager	<p>The following parameters are added:</p> <ul style="list-style-type: none"> ▪ export ▪ replace-ap
iot transportProfile	<p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ▪ ZSDFilter ▪ dataFilter <p>The following device class filters are introduced:</p> <ul style="list-style-type: none"> ▪ exposure-notification ▪ serial-data ▪ wiliot ▪ ZSD <p>The enableOnController parameter is removed.</p>
lc-cluster group-profile	The default value of the heartbeat-threshold parameter was changed to 900 ms.
logging	MAC-based debugging support in ISAKMPD is introduced. This feature will enable in debugging issues if APs are unable to form a tunnel with a controller in a scale setup.
mgmt-server	The ap-app-stats parameter is introduced.
provision-ap	The master-preference parameter was introduced.
rf arm-profile	<p>The following parameters were added:</p> <ul style="list-style-type: none"> ▪ cm-he-pooling-signal-delta ▪ cm-he-pooling-snr-thresh

Command	Description
show airgroup	The output of the show airgroup command is modified to include the new sub-parameter ppm under the parameter internal-state statistics .
show airgroupprofile	The output of the show airgroupprofile command is modified to include the following sub-parameters under the network default parameter: <ul style="list-style-type: none"> ▪ Enter MAC-Address or MAC-OUI to be blacklisted ▪ Configure max allowed IP per device. Default: 4 ▪ Configure max allowed tokens/cache per device (Default: 40)
show airmatch debug schedule	The output of the show airmatch debug schedule switch-info command is modified to include IPv6 address.
show ap active	The output parameters Radio 0 Band Ch/EIRP/MaxEIRP/Clients , Radio 1 Band Ch/EIRP/MaxEIRP/Clients , and Radio 2 Band Ch/EIRP/MaxEIRP/Clients include the following details: <ul style="list-style-type: none"> ▪ MPP: Indicates mesh-enabled radio of a mesh portal. ▪ MPC: The mesh point radio that has a parent link. ▪ MPA: The mesh point radio without a parent link.
show ap arm client-match history	The command output is modified to display information on clients having only IPv4 or IPv6 address, or a combination of both.
show ap database	The command displays two new flags, t and r to indicate Temperature Restriction and Power Restriction respectively.
show ap-group	The output is modified to include the following parameters: <ul style="list-style-type: none"> ▪ Mesh Accesslist Profile ▪ AirSlice Profile
show ap mesh active	The command displays a detailed output of all parameters only if mesh -enabled radios are configured.
show ap mesh neighbors	The output is modified to include the Radio parameter.
show ap mesh topology	The output is modified to include the Radio parameter.

Command	Description
show ap monitor	The following command outputs are modified to include ipv6 field: <ul style="list-style-type: none"> ▪ show ap monitor arp-cache ap-name <ap_name> ▪ show ap monitor debug status ap-name <ap_name> ▪ show ap monitor containment-info ap-name <ap_name>
show ap-name	The output is modified to include the following parameters: <ul style="list-style-type: none"> ▪ Mesh Accesslist Profile ▪ AirSlice Profile
show ap power-mgmt-statistics	The output is modified to display the ITM Status parameter.
show ap provisioning-profile	The output is modified to display the master preference of the AP.
show ap remote debug client-mgmt-counters	The following ASAP AP APP stats messages and record counters are introduced: <ul style="list-style-type: none"> ▪ total ▪ null sap ▪ empty ▪ error ▪ queued ▪ sent
show ap virtual-beacon-report	The command output is modified to also display IPv6 address of the AP.
show controller-ip	The command output is modified to display Switch IP as Switch IPv4 .
show datapath	The command outputs are modified to include the following: <ul style="list-style-type: none"> ▪ A new flag, X is introduced for show datapath tunnel command. ▪ The show datapath session dpi command displays the AirSlice ID.
show firewall	The output was modified to include the following parameters: <ul style="list-style-type: none"> ▪ Enable GRE Inner Frame Fragmentation ▪ Drop Larger than GRE MTU DF frame, send ICMP Err ▪ Drop Larger than GRE MTU DF frame ▪ Drop Larger than GRE MTU frame, send ICMP Err ▪ Drop Larger than GRE MTU frame

Command	Description
show gsm debug	The dual_controller_ip output parameter is introduced in the show gsm debug channel cluster command.
show gsm lookup	The output of the following commands are modified to display IPv6 address of the AP: <ul style="list-style-type: none"> ▪ show gsm lookup channel radio key radio_bssid <radio_bssid> ▪ show gsm lookup channel sta_mac_address <sta_mac_address>
show interface tunnel	The following parameters are introduced: <ul style="list-style-type: none"> ▪ Tunnel stats last fetched from SOS ▪ RxBytes:, TxBytes:, Encaps:, Decaps:
show iot-manager	The ble-services parameter is added.
show iot transportProfile	The following parameters are introduced: <ul style="list-style-type: none"> ▪ Zigbee Socket Device Filter ▪ Data Filter The following device class filters are introduced: <ul style="list-style-type: none"> ▪ exposure-notification ▪ wiliot ▪ ZSD The Enable BLE on Controller parameter is removed.
show ip access-list	The following parameters are introduced for VAPs in bridge mode: <ul style="list-style-type: none"> captiveportalbridge logon-control-bridge The global-geolocation-acl parameter is introduced.
show lc-cluster	The functionality of heartbeat counters parameter is modified.
show lc-rap-pool	The command output is modified to display IPv6 address used in Remote AP inner pool.
show master-local stats / show conductor-local stats	The output of the command is modified to include IPv6 address.
show memory	The as_visibility parameter is introduced.
show ssh	The hmac-sha2-256 parameter is introduced.
show upgrade managed-devices	The ca-bundle parameter is introduced.
show vlan-assignment	The IP Timeout Count and Time Full output parameters are introduced.

Command	Description
show vlan mapping	The IP Timeout , Max IP Timeouts and Full Period output parameters are introduced.
show whitelist-db cpsec-status/show allowlist-db cpsec-status	The output of the command is modified to include the following fields: <ul style="list-style-type: none"> ▪ My IPv6-Address ▪ Master IPv6-Address ▪ IPv6 LMS List
show wms rogue-ap	The output of the show wms rogue-ap <bssid> command is modified to display IPv6 address under Match IP field.
ssh	The command is modified to support SHA-2 authentication.
vlan-name	The ip-timeout , max-ip-timeouts and full-period sub-parameters are introduced.
vpnip	The v6 <vpncipv6> parameter is added.
web-server profile	TLS v1.2 is now the default ssl-protocol in the web-server profile. TLS v1 and TLS v1.1 is disabled by default.
wlan ssid-profile	The advertise-ap-name parameter is modified to include AP names in probe response frames.
upgrade managed-devices	The ca-bundle parameter is introduced.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.6.0.0.

New Commands in ArubaOS 8.6.0.0

The following commands were introduced in ArubaOS 8.6.0.0:

Command	Description
<u>aaa user-del-req-timeout</u>	This command configures the user delete request timeout value.
<u>ap convert</u>	This command converts Campus APs or Remote APs to Instant APs.
<u>ipv6 nexthop-list</u>	This command configures a next-hop list for IPv6 address in policy-based routing.
<u>policy-domain</u>	This command configures a policy domain profile to apply role-based ACL for users present in different controllers.
<u>replace-config-reboot</u>	This command replaces the configuration in a stand-alone controller and the controller will reboot with provided configuration file.
<u>secondary masteripv6/secondary conductoripv6</u>	This command adds a secondary Mobility Master containing IPv6 address.
<u>show aaa user-delete-result</u>	This command displays the list of users deleted for the last twenty delete requests issued from the managed devices.
<u>show ap power-mgmt-statistics</u>	This command shows the power status statistics of an AP connected to a managed device.
<u>show ipv6 nexthop-list</u>	This command displays the next-hop list settings for IPv6 address in policy-based routing.
<u>show policy-domain group-profile</u>	This command displays the details of the policy domain group profile.
<u>show ucc custom-sip</u>	This command displays the custom SIP ALG configuration.
<u>show ucc webrtc</u>	This command displays the WebRTC ALG configuration.
<u>vpn-acl</u>	This command configures both session and route ACL for branch-vpnc tunnel traffic.

Modified Commands in ArubaOS 8.6.0.0

The following commands were modified in ArubaOS 8.6.0.0:

Command	Description
aaa user delete	This command can now be executed from the Mobility Master using the ip-addr<ip-addr> and macaddr <macaddr> parameters.
airmatch ap	The values, 5GHzu for upper-band radios and 5GHzi for lower-band radios are supported by AP-555 access points.
ap mesh-ht-ssid-profile	The high-efficiency-enable parameter is introduced.
ap packet-capture	Radio ID 2 is introduced for AP-555 access points.
ap system-profile	The command is modified to include fast recovery mode on 530 Series and 550 Series APs. The sesimagotag-esl-servername parameter was added.
clear	The route-cache-v6 sub-parameter is introduced to the datapath parameter.
est	The following parameters are introduced, <ul style="list-style-type: none"> ▪ Arbitrary label enrollment ▪ Arbitrary label re-enrollment ▪ Organizational unit name ▪ Username /password
ids dos-profile	The spoofed death blacklist parameter is removed.
iot transportProfile	The following parameters are introduced: <ul style="list-style-type: none"> ▪ deviceCountOnly ▪ proxy ▪ rtIsDestMAC ▪ vendorFilter The following deviceClassFilters are introduced: <ul style="list-style-type: none"> ▪ abilitySmartSensor ▪ mysphera ▪ sbeacon ▪ wifi-assoc-sta

Command	Description
	<ul style="list-style-type: none"> ▪ wifi-tags ▪ wifi-unassoc-sta
ip access-list route	<p>The following configuration options are included under ipv6 parameter:</p> <ul style="list-style-type: none"> ▪ any ▪ host <ip-addr> ▪ network<ip-addr><netmask> ▪ route next-hop-list <next-hop-list-name>
license	<p>The <ipv6-addr> sub-parameter is added to the server-ip parameter.</p>
masteripv6/conductoripv6	<p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ▪ vpn-ipv6 <vpnipv6> ▪ peer-mac-1 <peermac-1> ▪ peer-mac-2 <peermac-2>
master-l3redundancy/conductor-l3redundancy	<p>The ipv6 <ipv6-addr> parameter is introduced.</p>
master-redundancy master-vrrp/conductor-redundancy conductor-vrrp	<p>The ipv6 <ipv6-addr> parameter is introduced.</p>
master-redundancy peer-ip-address/conductor-redundancy peer-ip-address	<p>The ipv6 <ipv6-addr> parameter is introduced.</p>
rf ht-radio-profile	<p>The bss-color-switch-count parameter is added.</p>
show airmatch debug apinfo	<p>The output parameters AP in Tri-Radio Mode and AP Tri-Radio Mode Last UpdTime are introduced for AP-555 access points.</p>
show airmatch debug nbr	<p>The output displays information about Radio 2 for AP-555 access points.</p>
show airmatch debug reporting-radio	<p>The output for AP-555 access points will display 5GHz Client count.</p>
show airmatch event	<p>The output displays information about Radio 2 for AP-555 access points.</p>
show airmatch solution	<p>The output displays information about Radio 2 for AP-555 access points.</p>

Command	Description
show ap active	The output parameter Radio 2 Band Ch/EIRP/MaxEIRP/Clients and flag t are introduced.
show ap arm client-match summary	The output of show ap arm client-match summary advanced will display the percentage of ClientMatch success in addition to the absolute values.
show ap arm client-match restriction-table	The output will display Client Restriction Table for Wifi2 for AP-555 access points.
show ap arm rf-summary	The output will display an interface report for Radio 2 for AP-555 access points.
show ap arm split-scan-history	The output will display an interface for Radio 2 for AP-555 access points.
show ap arm virtual-beacon-report	The output will display an interface report for Radio 2 for AP-555 access points.
show ap association	The output of this command is modified to include new flags for MBO and CDC feature for 802.11ax capable APs.
show ap bss-table	The output of this command is modified to include new flags for MBO and CDC feature for 802.11ax capable APs.
show ap bw-report	The output parameter Bandwidth report for AP "AP-Name" radio 2 is introduced for AP-555 access points.
show ap config	The output parameter 802.11a- secondary is introduced for AP-555 access points.
show ap debug airmatch	A new interface for Radio 2 will be displayed for AP-555 access points.
show ap debug anyspot-stats	Radio ID 2 is introduced for AP-555 access points.

Command	Description
<u>show ap debug power-table</u>	Radio ID 2 is introduced for AP-555 access points.
<u>show ap debug radio-info</u>	Radio ID 2 is introduced for AP-555 access points.
<u>show ap debug radio-registers</u>	Radio ID 2 is introduced for AP-555 access points
<u>show ap debug radio-stats</u>	Radio ID 2 is introduced for AP-555 access points.
<u>show ap debug received-config</u>	The output will display details of Radio 2 for AP-555 access points.
<u>show ap debug scan-settings</u>	The output will display the status of Radio 2 for AP-555 access points.
<u>show ap monitor</u>	<p>A new interface for Radio 2 will be displayed for the following parameters,</p> <ul style="list-style-type: none"> ▪ show ap monitor containment-info ▪ show ap monitor debug ▪ show ap monitor scan-info <p>The output of this command is modified to display bss color related information:</p> <ul style="list-style-type: none"> ▪ bss-color ▪ partial bss color ▪ bss color disabled
<u>show ap details</u>	The output parameter Radio 2 BSSID is introduced.
<u>show ap profile-usage</u>	The output will display the list of profiles associated to Radio 2 in AP-555 access points.
<u>show ap radio-database</u>	The output parameter Radio 2 Band Ch/EIRP/MaxEIRP/Clients is introduced.
<u>show ap remote debug bucketmap datapath</u>	The output will display tri-radio values for AP-555 access points.
<u>show ap spectrum debug</u>	The parameter radio {0 1 2} is introduced.

Command	Description
show ap spectrum debug monitors	The output displays the details of Radio 0, 1 and 2 for AP-555 access points.
show ap spectrum device-duty-cycle	The parameter radio {0 1 2} is introduced.
show ap standby	The output parameter Radio 2 Band Ch/EIRP/MaxEIRP/Clients and flag t are introduced.
show ap uac-database	The output parameter Radio 2 BSSID is introduced.
show database	The output of this command is modified to include IPv6 address of the peer Mobility Master in Layer-2 and Layer-3 redundancy.
show datapath	The remote-user table parameter is introduced.
show est profile	<p>The following parameters are introduced,</p> <ul style="list-style-type: none"> ▪ Arbitrary label enrollment ▪ Arbitrary label re-enrollment ▪ Organizational unit name ▪ Username /password <p>The following changes are introduced:</p> <ul style="list-style-type: none"> ▪ The ipv6 option is added to the nexthop-list sub-parameter. ▪ The output of the show datapath session ipv6 command is modified to display the next-hop list details, and includes the NhIdx, Nhidx, and NhNhVer columns. ▪ The output of the show datapath ipsec-map command is modified to display v6 value under IP ver column.
show threshold-limits	The no-of-vaps parameter is introduced to display the details of Virtual APs.

Command	Description
show gsm debug	The remote_ip_user parameter is introduced.
show iot transportProfile	The Vendor Filter , IoT Proxy Server , IoT Proxy User , Send device counts only , and RTLS Destination MAC Address parameters are introduced.
show license aggregate	The output displays IPv6 address under IP address parameter.
show license debug	The output displays the following new parameters: <ul style="list-style-type: none"> ▪ Master IPv6 ▪ Switch IPv6
show license heartbeat stats	The output displays IPv6 address under IP address parameter.
show license-usage	The output displays IPv6 address under IP address parameter.
show rf ht-radio-profile	The following output parameters are added: <ul style="list-style-type: none"> ▪ BSS Color ▪ BSS Color Switch Count
threshold	The no-of-vaps<value> parameter is introduced.
ucc	The custom-sip and webrtc parameters are introduced.
wlan ssid-profile	The cdc-enable and mbo-enable parameters are introduced.
wlan he-ssid-profile	The command is modified to support OFDMA, MU-MIMO, and TWT on all 802.11ax capable APs.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.5.0.0.

New Commands in ArubaOS 8.5.0.0

The following commands were introduced in ArubaOS 8.5.0.0:

Command	Description
<u>ap wifi-uplink-profile</u>	This command is introduced to configure a Wi-Fi uplink profile.
<u>controller-ble opmode</u>	This command is introduced to configure BLE opmode in controller.
<u>show ap debug ble-action-status</u>	This command is introduced to display action status for BLE devices seen by the AP.
<u>show ap wifi-uplink blacklist</u>	This command is introduced to display a list of Wi-Fi uplink APs that have been denied access.
<u>show ap wifi-uplink candidates</u>	This command is introduced to display a list of Wi-Fi uplink candidate APs.
<u>show ap wifi-uplink connection-history</u>	This command is introduced to display the connection history of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink connection-trace</u>	This command is introduced to display the connection trace of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink current-profile</u>	This command is introduced to display the current profile information of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink debug</u>	This command is introduced to display the debug information of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink neighbors</u>	This command is introduced to display the information of neighboring APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink-profile</u>	This command is introduced to display a list of all Wi-Fi uplink profiles, or display the configuration parameters in a specific Wi-Fi uplink profile.
<u>show ap wifi-uplink provisioned-profiles</u>	This command is introduced to display information of provisioned profiles of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink stats</u>	This command is introduced to display the statistics of APs with Wi-Fi uplink enabled.
<u>show ap wifi-uplink status</u>	This command is introduced to display the status of various parameters of APs with Wi-Fi uplink enabled.

Modified Commands in ArubaOS 8.5.0.0

The following commands were modified in ArubaOS 8.5.0.0:

Command	Description
aaa profile	The rfc-3576-server <ipaddr> parameter is updated to also support IPv6 address of the server.
aaa rfc-3576-server	The <ipaddr> sub-parameter is updated to also support IPv6 address of the server.
ap-group	The wifi-uplink-profile and enet0-usb-port-profile parameters are introduced.
ap system-profile	The rap-corp-dns-server and rap-corp-dns-server_ipv6 <ipv6 address> parameters are introduced.
crypto isakmp	The eap-gtc sub-parameter is introduced under the eap-passthrough parameter.
ids general-profile	The default value of max-monitored-devices parameter is modified to include both 1024 and 4096.
iot transportProfile	The aruba-sensors sub-parameter is introduced under the deviceClassFilter parameter.
interface tunnel	The keepalive icmp <ipaddr> <next-hop> parameter is introduced.
lc-cluster group-profile	The parameters, vrrp-id <starting id> and vrrp-passphrase <vrrp passphrase string> were added.
provision-ap	The link-priority-wifi and wifi-uplink parameters are introduced.
rf arm-profile	The cm-he-min-signal parameter is introduced.
rf am-scan-profile	The dwell-time-dos-channel parameter is introduced.
show ap active	A new flag, 4 is introduced to indicate Wi-Fi uplink.
show ap database	A new flag, 4 is introduced to indicate Wi-Fi uplink.
show ap-group	The Ethernet usb port configuration parameter is introduced.
show iot transportProfile	The aruba-sensors sub-parameter is introduced under the Device Class Filter parameter.
show lc-cluster	The load balance thresholds are updated and the Starting VRRP ID and VRRP Passphrase fields are added in the output.

Command	Description
show memory	The wcd sub-parameter is introduced under the ap parameter.
show wlan ssid-profile	The wpa3-aes-gcm-256 sub-parameter under the encryption parameter is introduced.
wlan ssid-profile	The refresh-direction parameter and the wpa3-aes-ccm-256 sub-parameter under the opmode parameter are introduced.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.4.0.0.

New Commands in ArubaOS 8.4.0.0

The following commands were introduced in ArubaOS 8.4.0.0:

Command	Description
ap ble-configure	This command is introduced to configure beacon attributes for a specific AP.
ap deep-sleep	This command is used to move the APs into deep-sleep mode.
ap provisioning-rule	This command is introduced to configure a group of APs and the subsequent actions to provision the APs.
ap provisioning-rules	This command is introduced to define the priority of the provisioning rules that are actively used by the Auto-provisioning feature in APs.
ap system-profile	The following parameters are added: <ul style="list-style-type: none">▪ <code>sesImagotag-esl-channel</code> - This parameter is introduced to configure the radio channel of SES-imagotag ESL system.▪ <code>sesImagotag-esl-serverip</code> - This parameter is introduced to configure the IP address of SES-imagotag ESL server.
ap wake-up	This command is used to wake up APs from the deep-sleep mode.
ap zeroize-tpm-keys	This command is introduced to erase the TPM content and render an AP permanently inoperable.
iapvpn-backward-compatible	This command is used to enable the older Instant APs to send register requests on the older HTTP port of 80.
iot radio-profile	This command is introduced to configure IoT radio profile.
ip domain redirect	This command is introduced to enable the DNS redirect feature.
ip domain-redirect	This command is introduced to redirect DNS query matching corporate domain to a dedicated corporate IPv4 DNS server.
ipv6 domain-redirect	This command is introduced to redirect the domain to a dedicated DNS server in the IPv6 domain.

Command	Description
<u>lc-cluster initiate schedule upgrade</u>	This command is introduced to schedule a cluster upgrade.
<u>lc-cluster initiate re-schedule upgrade</u>	This command is introduced to reschedule a scheduled cluster upgrade.
<u>lc-cluster initiate abort</u>	This command is introduced to delete or abort a scheduled cluster upgrade.
<u>password-recovery-disable</u>	This command is introduced to disable the default password recovery feature.
<u>password-recovery-user</u>	This command is introduced to create an alternate password recovery user.
<u>rf dot11-60GHz-radio-profile</u>	This command is introduced to configure AP radio settings for the 60 GHz frequency band, including the ARM profile for standalone controllers and the high-throughput (802.11ad) radio profile.
<u>show ap analytics recommendations</u>	This command is introduced to display the EIRP recommendations, channel-bandwidth recommendations, and regulatory domain profile recommendations to an AP.
<u>show ap ble-ibeacon-info</u>	This command displays the BLE ibeacon information for an AP.
<u>show ap debug esl-status</u>	This command displays the values for ESL Server, ESL Channel, ESL Radio, Configuration Status, and the ESL Dongle ID of an AP.
<u>show ap debug ses-esl-log</u>	This command displays the SES-Imagotog's ESL daemon debug logs for an AP.
<u>show ap greenap</u>	This command displays all the pending APs in the per-md list, sends the AP_INFO AMON message for a particular AP, and track Green AP related counters.
<u>show ap mesh debug link-table</u>	This command is introduced to display the mesh link table information for a remote mesh point or remote mesh portal.
<u>show ap provisioning-rule</u>	This command is introduced to display the information of an AP provisioning rule during Auto-provisioning..
<u>show ap provisioning-rules</u>	This command is introduced to display the information for the priority level of AP provisioning rules.
<u>show iot radio-profile</u>	This command displays the status of IoT radio profile.
<u>show provisioning-rule-info</u>	This command is introduced to display the information on each auto-provisioning rule and the associated APs.

Command	Description
show rf dot11-60GHz-radio-profile	This command displays an 802.11 60 GHz radio profile.
upgrade cancel-schedule	This command cancels an already scheduled upgrade of the managed devices.
upgrade reschedule	This command reschedules the existing scheduled upgrade of the managed devices.
vpn-peer pass-code	This command is introduced to configure authenticate code for automatic whitelisting of managed device on VPN Concentrators.
wlan he-ssid-profile	This command is introduced to configure a high-efficiency (802.11ax) SSID profile.
wmm-dscp-mapping	This command is introduced to enable the WMM DSCP map in the upstream direction of the decrypt-tunnel mode.
zeroize-tpm-keys	This command is introduced to erase the TPM content and render a controller permanently inoperable.

Modified Commands in ArubaOS 8.4.0.0

The following commands were modified in ArubaOS 8.4.0.0:

Command	Description
aaa authentication captive-portal	The ap-mac-in-redirect-url parameter is introduced.
aaa authentication via connection-profile	The I2-forwarding parameter is introduced.
ap-group	The dot11-60GHz-radio-profile parameter is introduced.
ap multizone-profile	<p>The following sub-parameters are introduced in the datazone parameter:</p> <ul style="list-style-type: none"> ▪ controller-ipv6 <ipv6> ▪ description <description> ▪ max-nodes <num_nodes> ▪ max-vaps <num_vaps> <p>The following sub-parameters are introduced in the primaryzone parameter:</p> <ul style="list-style-type: none"> ▪ max-nodes <num_nodes> ▪ max-vaps <num_vaps>

Command	Description
ap provisioning-profile	The apdot1x-tls-suffix , apdot1x-tls-suffix-domain , mesh-auto , and preferred_uplink parameters are introduced.
ap system-profile	<p>The following changes are introduced:</p> <ul style="list-style-type: none"> ■ The IPv6 address support is added to the ip-or-dns parameter. <p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ■ ap-usb-power-mode ■ wids-ampdu-optimization ■ seslmagotag-esl-channel ■ seslmagotag-esl-serverip <p>The following parameters are introduced:</p> <ul style="list-style-type: none"> ■ radio_5ghz_chain_4x4 ■ radio_5ghz_chain_5x5 ■ radio_5ghz_chain_6x6 ■ radio_5ghz_chain_7x7
ap wired-ap-profile	The wired-ap-mode parameter is introduced.
banner	The enforce-accept parameter is introduced.
ble_relay	The export-ap-ble-ibeacon-info parameter introduced.
interface tunnel	The vlan {add <word>} {remove <word>} <word> sub-parameters are introduced to the trusted parameter.
interface vlan	The pppoe-gateway-nat <nat-ip> sub-parameter is introduced.
iot transportProfile	<p>The following server types were introduced:</p> <ul style="list-style-type: none"> ■ Assa-Abloy ■ Meridian-beacons-management ■ Meridian-asset-tracking ■ Telemetry-https ■ Telemetry-websocket ■ ZF-openmatics <p>The following deviceClassFilters were introduced:</p> <ul style="list-style-type: none"> ■ all ■ aruba-beacons

Command	Description
	<ul style="list-style-type: none"> ▪ aruba-tags ▪ assa-abloy ▪ eddystone ▪ enoccean-sensors ▪ enoccean-switches ▪ ibeacon ▪ unclassified ▪ zf-tags <p>The following parameters were renamed from:</p> <ul style="list-style-type: none"> ▪ endpointType to serverType ▪ endpointID to clientID ▪ endpointURL to serverURL ▪ endpointToken to accessToken ▪ transportInterval to reportingInterval ▪ payloadContent to deviceClassFilter ▪ filterAttribute to uuidFilter ▪ namespaceFilter to uidNamespaceFilter ▪ cellSize to cellSizeFilter ▪ thresholdAttribute to movementFilter ▪ outrangeAgeout to ageFilter
ip access-list session	The output displays the use of source NAT to route the local traffic in AP datapath in Split-Tunnel forwarding mode for IPv6 clients.
ip dhcp pool	The switch-gw-ip sub-parameter is introduced.
ipv6 dhcp pool	The switch-gw-ipv6 sub-parameter is introduced.
lc-cluster group-profile	The parameter rapcluster is added.
mgmt-user	<p>The following sub-parameters are introduced in the <username> parameter:</p> <ul style="list-style-type: none"> ▪ max-concurrent-sessions ▪ old-password <p>The audit-period parameter is introduced.</p>

Command	Description
provision-ap	The apdot1x-tls-suffix , apdot1x-tls-suffix-domain , mesh-auto , and preferred_uplink parameters are introduced.
rf dot11a-radio-profile	The high-efficiency-enable <radio> parameter is introduced.
rf dot11g-radio-profile	The high-efficiency-enable parameter is introduced.
rf ht-radio-profile	The bss-color parameter is introduced.
show airgroup aps	The output is modified to display the name of the neighbor AP, if available, in the Neighbor AP name parameter.
show aaa authentication via connection-profile	The output of this command is modified to display the Use I2 forwarding parameter.
show aaa radius-attributes	The output of this command is modified to display Aruba-Captive-Portal-URL VSA attribute.
show amon-sender	The following new parameters are added to support Smart AMON feature: <ul style="list-style-type: none"> ▪ bundle counters ▪ bundle parameters ▪ cdt message-type
show ap database	A new flag, p was introduced to show that the AP is in deep-sleep mode.
show ap debug multizone	The output of this command is modified to include V flags.
show ap details	The following changes are introduced: <ul style="list-style-type: none"> ▪ The output of the show ap details advanced ip-addr <ip-addr> command is modified to display a new field, Reason for disconnect. ▪ The output of the show ap details advanced ap-name <ap-name> command is

Command	Description
	modified to display Eirp (max, min, offset) information.
show ap-group	The output of this command is modified to display the 802.11 60GHz radio profile parameter and its corresponding value.
show ap mesh debug forwarding-table	The ssid parameter was introduced.
show ap monitor debug	The following changes are introduced: <ul style="list-style-type: none"> ▪ The ip6-addr parameter is added. ▪ The output of the show ap monitor debug status command displays both IPv4 and IPv6 addresses. ▪ The output of the show ap monitor debug status command includes the new counters to differentiate the distribution of DATA, MGMT, CTRL, and AGGR packets.
show ap monitor stats	The output of the show ap monitor stats command is modified to display the additional debug counter information.
show ap multizone-profile	The output is modified to display the IPv6 Address and Description columns.
show ap provisioning-profile	The output is modified to include the following parameters: <ul style="list-style-type: none"> ▪ AP dot1x EAP-TLS username suffix ▪ AP dot1x EAP-TLS username suffix domain ▪ USB power mode
show ap system-profile	The following changes are introduced: <ul style="list-style-type: none"> ▪ The output of the show ap system-profile <profile-name> include USB

Command	Description
	<p>command displays the AP USB Power mode parameter.</p> <ul style="list-style-type: none"> ▪ The AeroScout RTLS Server and RTLS Server configuration output parameter of the show ap system-profile <profile-name> include RTLS command displays IPv6 address.
show audit-trail	The output displays international characters in the ESSID, in unicode format.
show datapath	<p>The following changes are introduced:</p> <ul style="list-style-type: none"> ▪ The output of the #show datapath tunnel ipv6 command was modified to include B, G, and Y flags. ▪ The outputs of the show datapath route ap-name <ap-name> ipv6 and show datapath route-cache ap-name <ap-name> ipv6 commands are modified to display IPv6 route entries. ▪ The web-cc and counters sub-parameters are added to ipv6 parameter. ▪ The output of the show datapath session ipv6 web-cc command is modified to display WebCC related entries for IPv6 sessions. ▪ The trusted-vlan and untrusted-vlan sub-parameters are introduced in the show datapath tunnel tunnel-id <id> command.
show gsm debug	The via_user and rap-pubic-ip sub-parameter is introduced in the <channel> parameter.

Command	Description
show lc-cluster	This scheduled-upgrades and rap-public-ip parameter is introduced.
show license-usage	The Active MUX and Active PUTN parameters were added.
show mgmt-user	The following parameters are introduced: <ul style="list-style-type: none"> ▪ audit-info ▪ console The Max-concurrent-sessions parameter is introduced in the output.
show provisioning-params	The output is modified to include the following parameters: <ul style="list-style-type: none"> ▪ AP dot1x EAP-TLS username suffix ▪ AP dot1x EAP-TLS username suffix domain
show rights	The output displays the IPv6 ACE entries of role-based ACL in Split-Tunnel forwarding mode.
show tpm	The errorlog parameter is introduced.
show via	The lastlogin parameter is introduced.
show interface tunnel	The trusted-vlan and untrusted-vlan sub-parameters are introduced.
show ip pppoe-info	The output of the show ip pppoe-info command is modified to display Gateway NAT and IP parameters.
show sapm cluster nodestate	The Public IP address output column was added.
show web-cc	The output of the show webcc-status command displays the Connection mode for server parameter.
upgrade managed-devices	The schedule parameter is introduced.
webcc	The connectiontype ipv6 parameter is introduced.

Command	Description
wlan ssid-profile	The enhanced-open , wpa3-aes-ccm-128 , wpa3-cnsa , and wpa-sae-aes sub-parameters are introduced to the opmode parameter and the opmode-transition parameter is introduced.

Deprecated Commands in ArubaOS 8.4.0.0

The following commands were deprecated in ArubaOS 8.4.0.0:

Command	Description
panic	This command managed information created during a system crash.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.3.0.0.

New Commands in ArubaOS 8.3.0.0

The following commands were introduced in ArubaOS 8.3.0.0:

Command	Description
iot transportProfile	This command configures an IoT transport profile.
iot usetransportProfile	This command sets an IoT management server profile.
show iot transportProfile	This command displays information about the IoT profile status.
show airmatch debug apinfo	This command displays information about the AirMatch debug data of an AP.
show airmatch debug db-dump status	This command displays information about the status of the AirMatch debug database dump.
show airmatch debug pathloss history rep-radio	This command displays information about the recent AirMatch debug path loss.
show airmatch network-tech-support	This command collects the output for all the radios that are in the same partition for a specified radio AP name.
show airmatch tech-support	Displays the AirMatch technical support information of an AP.
show airmatch debug advanced stat	This command displays detailed information about the AirMatch debug status of an AP.
show ble_relay disp-attr	This command shows the BLE relay attributes.
show ble_relay iot-profile	This command shows the BLE relay IoT profile details.
show ble_relay tag-report	This command shows the BLE relay tag data.
show ble_relay ws-log	This command shows the BLE relay WebSocket logs.

Modified Commands in ArubaOS 8.3.0.0

The following commands were modified in ArubaOS 8.3.0.0:

Command	Description
aaa authentication via connection-profile	The following changes are introduced: <ul style="list-style-type: none">▪ A new parameter, tos-dscp, is introduced to support IPsec packets with higher QoS-DSCP.

Command	Description
	<ul style="list-style-type: none"> The description of the whitelist parameter is updated to display the maximum limit of allowable entries.
aaa profile	<p>The following new parameters are introduced:</p> <ul style="list-style-type: none"> radius-acct-session-id-in-access reauth-wired-user-vlan-change
ap system-profile	<p>The following new parameters are introduced:</p> <ul style="list-style-type: none"> dual-5ghz-mode recovery-mode
ap wired-port-profile	<p>The following new parameters are introduced:</p> <ul style="list-style-type: none"> auto-recovery-enable auto-recovery-interval loop-detection-interval loop-protect-enable
configuration device	<p>The A7280 option is added under the device-model parameter.</p>
provision-ap	<p>The following parameters are introduced:</p> <ul style="list-style-type: none"> radio-0-5ghz-ant-gain radio-0-5ghz-ant-pol radio-1-5ghz-ant-gain radio-1-5ghz-ant-pol
show ap active	<p>The new flags, T, U, V, and W are introduced. In addition, the output parameters for this command are modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation modes for the dual 5GHz mode settings.</p>
show ap arm client-match history	<p>A new output value, AS is introduced for the Signal output column.</p>
show ap arm client-match summary	<p>A new parameter, brief, is introduced to display brief statistical information of the output parameters.</p>
show ap details	<p>The output of the command is modified to include AP Fast Recovery statistics.</p>
show airmatch debug feasibility	<p>The following parameters are introduced in the output of this command:</p> <ul style="list-style-type: none"> Current Opmode HW Supported Opmodes Configured Opmodes Feasible Opmodes

Command	Description
	<ul style="list-style-type: none"> ▪ Config BW range(MHz) ▪ Hardware BW range(MHz) ▪ Eirp Range Chan 20MHz ▪ Eirp Range Chan 40MHz ▪ Eirp Range Chan 80MHz ▪ Eirp Range Chan 160MHz ▪ Config EIRP range(dBm) ▪ Hardware EIRP range(dBm) ▪ EIRP Offset(dB) ▪ Band ▪ Band Range
<u>show ap debug radio-stats</u>	The output of this command includes MCS bucket mapping information with channel width, number of spatial streams, and guard interval information of 802.11ac APs.
<u>show ap debug bss-stats</u>	
<u>show ap debug client-stats</u>	
<u>show ap wired-port-profile</u>	<p>The following parameters are introduced in the output of this command:</p> <ul style="list-style-type: none"> ▪ Loop Protect Enable ▪ Loop Detection Interval ▪ Loop Protect Auto Recovery Enable ▪ Loop Protect Auto Recovery Interval
<u>show datapath</u>	The current standby entries counter is added to the station parameter.
<u>ssh</u>	The disable-ciphers and disable-mac parameters have been introduced in this command to configure ciphers and MAC algorithms, respectively.
<u>show ssh</u>	The ssh disable-ciphers and ssh disable-mac parameters are introduced to the output of this show command.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.2.2.0.

New Commands in ArubaOS 8.2.2.0

The following commands were introduced in ArubaOS 8.2.2.0:

Command	Description
show airmatch debug advanced stat	This command displays detailed statistics about the APs or radios on a Mobility Master.
show airmatch debug db-dump status	This command displays information about the status of the AirMatch debug database dump.
show airmatch network-tech-support	This command collects the output for all the radios that are in the same partition for a specified radio AP name. This command also lists and describes the AP radios that will be handled further.
show airmatch tech-support	This command collects the output for the AP or the radio, of a series of related AirMatch commands.

Modified Commands in ArubaOS 8.2.2.0

The following commands were modified in ArubaOS 8.2.2.0:

Command	Description
banner	The enforce-accept parameter is introduced.
mgmt-user	The following sub-parameters are introduced in the <username> parameter: <ul style="list-style-type: none">▪ max-concurrent-sessions▪ old-password The audit-period parameter is introduced.
show mgmt-user	The following parameters are introduced: <ul style="list-style-type: none">▪ audit-info▪ console The Max-concurrent-sessions parameter is introduced in the output.
show tpm	The errorlog parameter is introduced.
show via	The lastlogin parameter is introduced.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.2.1.0.

New Commands in ArubaOS 8.2.1.0

The following commands were introduced in ArubaOS 8.2.1.0:

Command	Description
<u>show airmatch debug advanced stat</u>	This command displays detailed statistics about the APs or radios on a Mobility Master.
<u>show airmatch debug db-dump status</u>	This command displays information about the status of the AirMatch debug database dump.
<u>show airmatch tech-support</u>	This command collects the output for all the radios that are in the same partition for a specified radio AP name. This command also lists and describes the AP radios that will be handled further.
<u>show airmatch network-tech-support</u>	This command collects the output for the AP or the radio, of a series of related AirMatch commands.

Modified Commands in ArubaOS 8.2.1.0

The following commands were modified in ArubaOS 8.2.1.0:

Command	Description
<u>clear</u>	The web-cc parameter is introduced.
<u>ip dhcp pool</u>	Support for specifying option code with hex data string is introduced.
<u>ntp authentication-key</u>	The sha1 parameter is introduced.
<u>rf dot11a-radio-profile</u>	The 300 Series access points disregards the value configured for the cell-size-reduction parameter.
<u>rf dot11g-radio-profile</u>	The 300 Series access points disregards the value configured for the cell-size-reduction parameter.
<u>show ip ospf</u>	The Tx Err and Rx Err parameters are added to the output of the show ip ospf interface vlan command.
<u>show ip route</u>	The order of displaying the administrative distance and cost is changed to [AD/Cost] from [Cost/AD] in the command output.
<u>show netdestination</u>	The Destination ID parameter is added to the command output.
<u>show ntp authentication-keys</u>	The output of this command is modified to show the SHA1 key type and secret (in encoded format), when SHA1 authentication is configured.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.2.0.0.

New Commands in ArubaOS 8.2.0.0

The following commands were introduced in ArubaOS 8.2.0.0:

Command	Description
<u>airgroupprofile</u>	This command is used to configure an AirGroup profile.
<u>ap deploy-profile</u>	This command is used to enable and configure policies on the AP deploy profile. The AP deployment policy redirects the selected APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.
<u>ap redeploy controller-less</u>	The command sets the AP preference role to controller-less. APs with the controller-less preference role bypass controller discovery and immediately initiate Instant discovery.
<u>configuration rename</u>	This command is used to rename a node path.
<u>est</u>	This command is used to configure an EST profile on the controller or the AP for certificate enrollment.
<u>est-activate</u>	This command is used to activate an EST profile configured on the controller or the AP.
<u>ip dhcp increase-lease-limit</u>	This command configures additional DHCP scope that is twice the user limit on specific controller (that is, 7005 controller, 7008 controller, and 7010 controller) platforms.
<u>ipv6 helper-address</u>	This command enables the slog_flash application.
<u>master-l3redundancy/conductor-l3redundancy</u>	This command is used to configure Layer-3 redundancy for a Mobility Master.
<u>secondary masterip/secondary conductorip</u>	This command is used to configure a secondary master-ip.
<u>show ap deploy-profile</u>	This command displays the policies configured and the status of the AP deploy profile.
<u>show est status</u>	This command displays the current status of the EST profile configured on the device and optionally provides details of the EST on the consolidated list of switches.
<u>show master-l3redundancy/show conductor-l3redundancy</u>	This command displays the current status of Layer-3-domain Mobility Master redundancy. (

Command	Description
show scp	This command shows the SCP server functionality status of the controller or managed device.
show uap-blacklist/show uap-denylist	This command displays the Unified AP (UAP) blacklist database entries.
show wired-blacklist-clients/show wired-denylist-clients	This command shows the blacklisted wired clients.
show wms rogue-ap list	This command shows the list of rogue APs in the WMS.
uap-blacklist / uap-denylist	This command allows you to create, modify, delete, or purge a blacklist database on the device.
webcc	This command changes the WebCC operational mode from the default centralized mode to distributed mode for the managed device. In distributed mode, the managed device contacts the cloud WebRoot server for URL lookup queries as opposed to the Mobility Master in the default centralized mode.

Modified Commands in ArubaOS 8.2.0.0

The following commands were modified in ArubaOS 8.2.0.0:

Command	Description
aaa authentication wired	The blacklist-time parameter is added.
aaa rfc-3576-server	Event-timestamp-required , replay-protection , and window-duration parameters are added.
aaa timers	The range of stats-timeout parameter is updated to 5-60 minutes.
airmatch ap	The eirp parameter supports the configuration of EIRP values in .1 dBm increments. EIRP values for 270 Series access points can be configured as a negative value.
ap provisioning-profile	The apdot1x-factory-cert and apdot1x-tls parameters are added.
ap system-profile	The following changes are introduced to the ipm power-reduction-step-priority parameter: <ul style="list-style-type: none"> ▪ The all sub-parameter is added to remove all IPM steps or priorities by executing a single command. ▪ The priority parameter is not required now to delete a single IPM step/priority. You only

Command	Description
	<p>need to provide the ipm-step.</p> <ul style="list-style-type: none"> The following new parameters are introduced: disable_pse, radio_2ghz_chain_1x1, radio_2ghz_chain_2x2, radio_2ghz_chain_3x3, radio_2ghz_power_3dB, radio_2ghz_power_6dB, radio_5ghz_chain_1x1, radio_5ghz_chain_2x2, radio_5ghz_chain_3x3.
configuration node	The move-to sub-parameter is introduced under the <node-path> parameter.
crypto-local ipsec-map	The enrolled-cert-auth parameter is added to enable enrolled certificate authentication for site-to-site tunnel.
interface cellular	Updated the new syntax as ip access-group session <name>
interface gigabitethernet	Updated the new syntax as ip access-group {in out session {vlan <vlanId>}} <name>
interface port-channel	<p>The following changes are introduced:</p> <ul style="list-style-type: none"> Updated the new syntax as ip access-group {in out session {vlan <vlanId>}} <name> A new sub parameter <WORD> is introduced under switchport trunk allowed parameter. You can specify none to remove all the VLANs from the list of allowed VLANs configured on the trunk port.
interface port-channel	Updated the new syntax as ip access-group {in out session {vlan <vlanId>}} <acl_name> .
interface tunnel	Updated the new syntax as ip access group in <acl-name> .
interface vlan	Updated the new syntax as ip access-group in <acl_name> .
ipv6 domain lookup	The lookup parameter is added.
ipv6 name-server	The domain server IPv6 address is added.
ipv6 mld	The max-members-per-group parameter is added.
logging	New system processes called vrrp and lagm are added to debug issues related to vrrp and lacp in GSM channels respectively.
provision-ap	The apdot1x-factory-cert and apdot1x-tls parameters are added.

Command	Description
rf dot11a-radio-profile	The following parameters only appear in the command-line interface of Mobility Master, and are not configurable via a standalone controller <ul style="list-style-type: none"> ▪ deploy-hour ▪ eirp-max ▪ eirp-min ▪ eirp-offset
rf dot11g-radio-profile	<ul style="list-style-type: none"> ▪ energy-detect-threshold ▪ max-channel-bandwidth <p>The following parameter is only available in the command-line interface of a standalone controller, and is not configurable via Mobility Master.</p> <ul style="list-style-type: none"> ▪ channel
service	The scp parameter is introduced. This parameter enables the scp server functionality on the controller or managed device.
show aaa bandwidth-contracts	The dynamic parameter is added.
show airmatch debug feasibility	The output in the EIRP field can display EIRP values in .1 dBm increments, and the Update Reason field can show if an AirMatch update was made due to a radio band change by an AP radio that supports both 1x1 dual radio mode and 2x2 single radio mode (flex-mode).
show airmatch debug history	The output in the EIRP fields of these commands can display EIRP values in .1 dBm increments.
show airmatch debug reporting-radio	
show ap system-profile	The output of the command has a new parameter, IPM Steps delete all .
show ip domain-name	The IPv6 domain lookup parameter is added.
show configuration	A new parameter, filtered , is added to show the configuration downgraded to other versions. That is, it shows the configurations that are removed from the merged configuration before sending to a device.
show datapath	A new parameter, netdest-id , is added to show the datapath ACL netdestination table for AP name, IP address of AP, or ID.
show gsm debug	The sectun parameter accepts IPv6 addresses.
show interface vlan	The IPv6 helper-address is displayed in the output.
show ip dhcp	The output of this command is modified to display a warning message if the configured DHCP lease limit exceeds the maximum user limit defined.

Command	Description
<u>show license client-table</u>	The output of these commands display information for VIA licenses introduced in ArubaOS 8.2.0.0.
<u>show license server-table</u>	
<u>show ucc call-info cdrs</u>	The Server (IP) parameter is added.
<u>show upgrade-profile</u>	The serveraddr parameter is added.
<u>show web-cc</u>	The output of this command is enhanced to display information for WebCC license features configured in centralized or distributed mode.
<u>upgrade managed-devices</u>	The imagehost parameter accepts IPv6 address of the image server.
<u>upgrade-profile</u>	The serveraddr parameter accepts IPv6 address of the image server.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.1.0.0.

New Commands in ArubaOS 8.1.0.0

The following commands were introduced in ArubaOS 8.1.0.0:

Command	Description
aaa radius modifier	This command configures the RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server.
lb-group	This command manages and configures the load balancing group.
lc-cluster initiate initiate Upgrade	This command is used to upgrade a cluster.
show aaa radius modifier	This command displays all the RADIUS modifier profiles.
show airmatch optimization	This command displays list of recent RF optimization jobs performed by AirMatch, and displays statistics that determine the overall quality of the optimization change.
show running-config	This command displays the current Mobility Master configuration, including all pending changes that are yet to be saved.
show tunneled-node-mgr	This command displays the tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Modified Commands in ArubaOS 8.1.0.0

The following commands were modified in ArubaOS 8.1.0.0:

Command	Description
aaa authentication-server radius	The acct-modifier and auth-modifier parameters are introduced.
aaa authentication via auth-profile	The client-cert-enable parameter is introduced.
aaa authentication via connection-profile	The certificate-criteria parameter is introduced.
aaa profile	The radius-roam-accounting parameter is introduced.
aaa test-server	The verbose option is introduced.
amon msg-buffer-size	The msg-buffer-size range is modified.
ap multizone-profile	The primaryzone parameter was introduced.

Command	Description
airmatch profile	The eirp-offset parameter is removed from this command. This parameter is introduced into the rf dot11a-radio-profile and rf dot11g-radio-profile commands to support greater flexibility in configuring EIRP levels.
crypto-local ipsec-map	The any sub-parameter is introduced in dst-net , and src-net parameters. . The client-mode , load-balance , and monitor parameters are introduced.
crypto ipsec	The esp-null transform-set parameter is introduced.
ipv6 proxy-ra	The proxy-ra parameter is modified to enable proxy router advertisements.
logging	The format parameter is introduced to allow cef or bsd-standard logging formats.
mgmt-server	The following changes were introduced: <ul style="list-style-type: none"> ▪ The primary-server parameter is modified to accept IPv6 address. ▪ The Clarity Live parameters such as inline-ap-stats, inline-auth-stats, inline-dhcp-stats, and inline-dns-stats are introduced. ▪ The secure and transport parameters are introduced to specify the use of DTLS mode.
mgmt-user	The standard role is introduced.
ntp	The server-mode and source parameters are introduced.
ping	The following parameters are introduced: <ul style="list-style-type: none"> ▪ interval ▪ ttl ▪ validate-reply
provision-ap	The server-ip parameter is modified to accept IPv6 address.
rf dot11a-radio-profile	The deploy-hour parameter is introduced to set the hour during which AirMatch updates are sent to the APs using that radio profile. If this parameter is set in both the AirMatch profile and the 5 GHz (802.11a) radio profile, the setting in the 5 GHz radio profile will take precedence. The eirp-offset parameter is introduced to modify EIRP levels selected by the AirMatch algorithm. The energy-detect-threshold parameter is introduced to modify the Energy Detect Threshold (EDT) used by the AP radio in making transmit decisions. The minimum-channel-bandwidth parameter is introduced to set the minimum channel bandwidth for 802.11a radios on APs associated to Mobility Master managed devices.

Command	Description
rf dot11g-radio-profile	<p>The deploy-hour parameter is introduced to set the hour during which AirMatch updates are sent to the APs using that radio profile. If this parameter is set in both the AirMatch profile and the 5 GHz (802.11a) radio profile, the setting in the 5 GHz radio profile will take precedence.</p> <p>The airp-offset parameter is introduced to modify EIRP levels selected by the AirMatch algorithm.</p> <p>The energy-detect-threshold parameter is introduced to modify the Energy Detect Threshold (EDT) used by the AP radio in making transmit decisions.</p> <p>The minimum-channel-bandwidth parameter is introduced to set the minimum channel bandwidth for 2.4 GHz (802.11g) radios on APs associated to Mobility Master or managed devices.</p>
router ospf	The static sub-parameter is introduced under the redistribute parameter.
show aaa profile	The RADIUS Roaming Accounting parameter is introduced.
show airmatch solution	The output of this command has been modified in ArubaOS 8.1. This command now displays history of AirMatch solution updates, including the previous and updated channel and EIRP values. The capacity , cost and conflict values that appeared in the output in previous versions of this command now appear in the output of the command show airmatch optimization .
show amon-sender	<p>The following parameters are modified to accept IPv6 address:</p> <ul style="list-style-type: none"> ▪ dest-stats-all ▪ dest-stats-inst-0-7 ▪ interest-table
show gsm debug	The tunneled_node and tunneled_user parameter are introduced.
show ipv6 ra	The proxy parameter is introduced.
show mgmt-servers	This command lists primary servers with IPv6 address.
uplink	The load-balance and wired parameters are introduced.
web-server profile	The via-client-cert-port parameter is introduced.

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.0.1.0.

New Commands in ArubaOS 8.0.1.0

The following commands were introduced in ArubaOS 8.0.1.0:

Command	Description
airmatch db-dump	This command creates a dump of the database used by AirMatch. The dump file can be exported using the copy command.
crypto-local isakmp allow-via-subnet-routes	This command allows VIA clients to push subnet routes to Mobility Master.
papi-security	The papi-security command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.
show ip-flow-export wireless-cache	The show ip-flow-export wireless-cache command displays the cache for WLAN information.
show papi-security	The show papi-security command shows a configured papi-security profile.
show websocket	The show websocket command displays the ClearPass WebSocket configuration.

Modified Commands in ArubaOS 8.0.1.0

The following commands were modified in ArubaOS 8.0.1.0:

Command	Description
airmatch ap	The lms lms-ip <lms-ip> and lms lms-ipv6 <lms-ipv6> parameters are introduced, to allow you to freeze or unfreeze AP channels on a local controller.
airmatch profile	The quality-threshold parameter is introduced, which allows you to select a percentage of potential channel improvement that will trigger a new channel solution.
airmatch db-dump	This command creates a dump of the database used by AirMatch. The dump file can be exported using the copy command.
ap multizone-profile	The num-nodes sub-parameter is introduced.
ip-flow-export-profile	The wireless-export parameter is introduced.
interface mgmt	vlan-tag optional sub-parameter is introduced under the ip address and ipv6 address parameters.

Command	Description
<u>logging</u>	The logging level <severity> is moved to the end of the command string.
<u>license</u>	The server-ip parameter is introduced to configure a standalone controller as a licensing client.
<u>mgmt-user</u>	The node parameter is introduced in the mgmt-user <username> <rolename> command.
<u>show ap multizone-profile</u>	The num-nodes sub-parameter is introduced.
<u>show crypto-local isakmp</u>	The allow-via-subnet-routes sub-command is introduced.
<u>show ipc statistics app-name</u>	Tx Sign, Rx Sign, and Rx Denied columns are added to the command output.
<u>show license-usage</u>	The verbose parameter is added to display license usage statistics for individual license pools and the devices associated to those license pools.

The following is the list of terminologies used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11i. The difference between bSec and standard 802.11i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11a provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises.

This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

app

Short form for application. It generally refers to the application that is downloaded and used on mobile devices.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID

is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension

formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CLI

Command-Line Interface. A console interface with a command line shell that allows users to execute text input as commands and convert these commands to appropriate functions.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the "common name", which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP–Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP–Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP–Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format: APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GARP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

gateway

Gateway is a network node that allows traffic to flow in and out of the network.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the w servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP-Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

netmask

Netmask is a 32-bit mask used for segregating IP address into subnets. Netmask defines the class and range of IP addresses.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

onboarding

The process of preparing a device for use on an enterprise network, by creating the appropriate access credentials and setting up the network connection parameters.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on polices configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control Information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

Power On Self Test. An HTTP request method that requests data from a specified resource.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deployed at branch office sites and are connected to the central network on a WAN

link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documents.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

subscription

A business model where a customer pays a certain amount as subscription price to obtain access to a product or service.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UI

User Interface.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnP is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only

pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.